OpenShift Roadmap Update: What's Next?

August 2018 update

Product Management

OpenShift Roadmap

Q2 CY2018

OpenShift Container Platform 3.10 (July)

- Kubernetes 1.10 and CRI-O option
- Smart Pruning
- Istio (Dev Preview)
- oc client for developers
- Control plane as static pods and TLS bootstrapping
- Windows Server Containers (Dev Preview))
- Prometheus Metrics and Alerts (Tech Preview)
- S3 Svc Broker

OpenShift Online & Dedicated

- Dedicated self-service: RBAC, limit ranges
- Dedicated encrypted storage, multi-AZ, Azure beta

Q3 CY2018

OpenShift Container Platform 3.11 (Oct)

- Kubernetes 1.11 and CRI-O option
- Infra monitoring, alerting with SRE intelligence, Node Problem Detector
- Etcd and Prometheus Operators (Tech Preview)
- Operator Certification Program and JBoss Fuse Operator
- P-SAP features
- Metering and Chargeback (Tech Preview)
- HPA Custom Metric
- OLM & Operator Framework (Tech Preview)
- New web console for developers and cluster admins
- Ansible Galaxy ASB support
- CNV (Developer Preview)
- OVN (Tech Preview for Windows)
- FISMA Moderate, ISO27001 PAGs, PCI-DSS Reference Architecture

OpenShift Online & Dedicated

- OpenShift Online automated updates for OS
- Chargeback (usage tracking) for OpenShift Online Starter

Q1 CY2019

OpenShift Container Platform 4.0 (March)

- Kubernetes 1.12 and CRI-O default
- Converged Platform
- Full Stack Automated Installer
  - AWS, OSP (tentative)
- Over-The-Air Updates
- RHCC integrated experience
- Windows Containers Tech Preview
- Easy/Trackable Evaluations
- Red Hat CoreOS as immutable host option
- Cluster Registry
- HPA custom metrics from Prometheus (Tech Preview)
- FIPS mode for golang (Dev preview)
- OVN Tech Preview

OpenShift Online & Dedicated

- Cluster Operator driven installs
- Self-Service Dedicated User Experience

Q2 CY2019

OpenShift Container Platform 4.1 (July)

- Kubernetes 1.13 and CRI-O default
- Full Stack Automated Installer
  - OSP, Azure
- Istio GA
- Mobile 5.x
- Serverless (Tech Preview)
- RHCC for non-container content
- Integrated Quay (Tech Preview)
- Idling Controller
- Federated Ingress and Workload Policy
- OVN GA
- Che (Tech Preview)

OpenShift Online & Dedicated

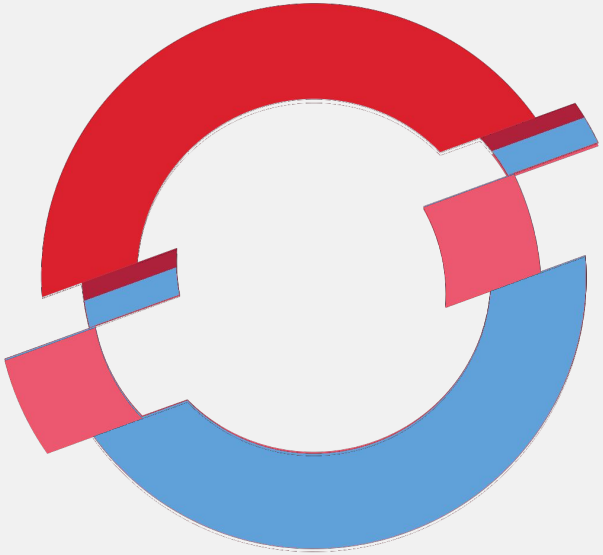
- OpenShift.io on Dedicated (Tech Preview)

redhat.

OpenShift 4

A Simple , Automated Platform for the Hybrid Cloud

1. Operator Enabled Platform
2. One Unit of Automation
3. Integrated Marketplace

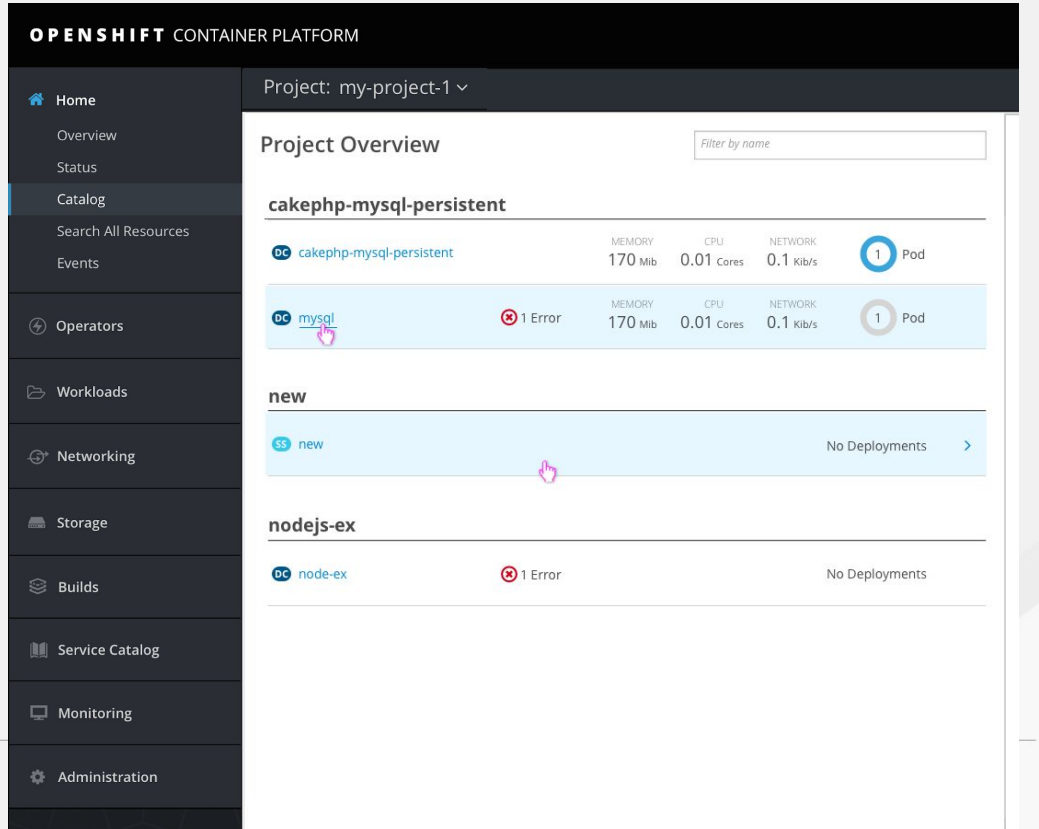


Developer Experience

App Developer & Cluster Admin Console

TARGET FOR 4.0

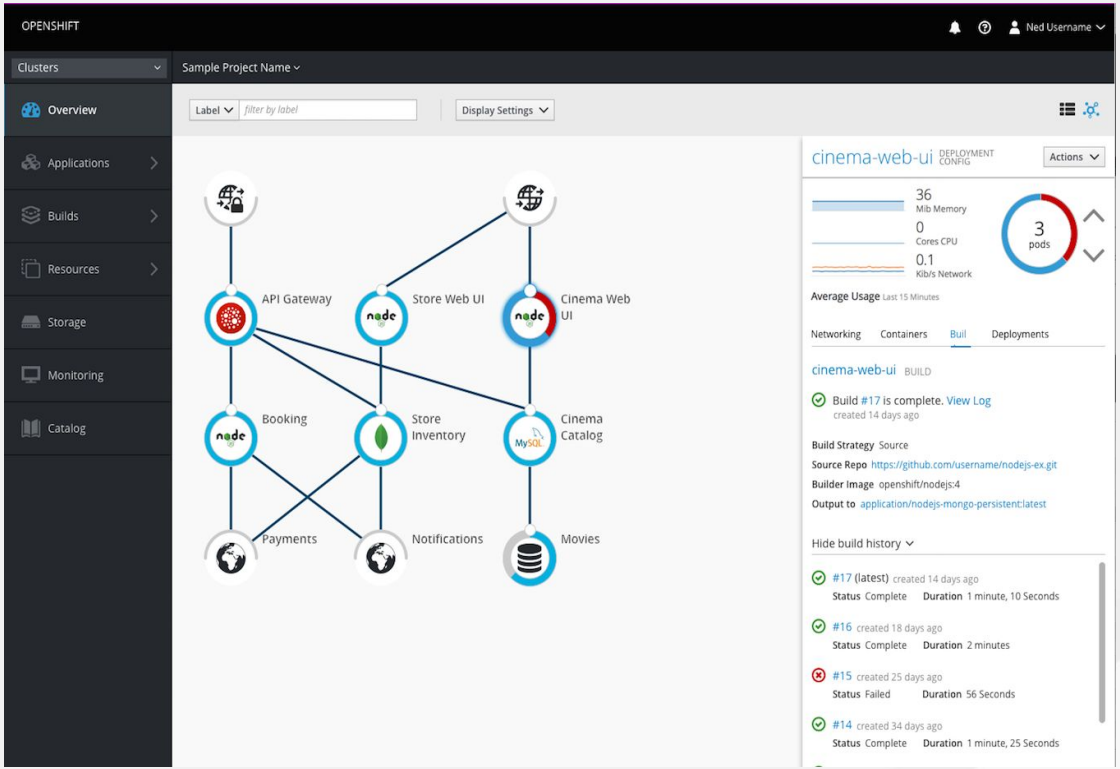
- Unified web console
- Tailored towards app dev and admin personas
- Redesigned catalog and overview experience
- Better categorization & discovery for source-to-image
- Exposing more CaaS



Application Focused UX

TARGET FOR 4.1

- Organize applications based on grouping labeled components
- Leverage owner references and network connectivity
- Include higher level statistics



Building Container Images

- docker 1.13 last supported upstream “docker” in Kubernetes
- Already a high burden maintaining a secure platform based on docker daemon model
- Increased burden in Kubernetes with aging container runtime

- In comes cri-o and buildah to the rescue
- Update s2i to generate Dockerfile, piped into buildah

- Growing number of docker-less options

cri-o

buildah

Source-to-Image

OPENSHIFT-DO: A CLI FOR DEVELOPERS

Openshift-DO ("odo") is a new CLI plugin for OpenShift 3.9+ that is tailored for developer syntax and workflows.

Goal is to make it simple for a developer to create an app, add components (like a database) and expose it without needing to know Kubernetes.

In tech preview now.

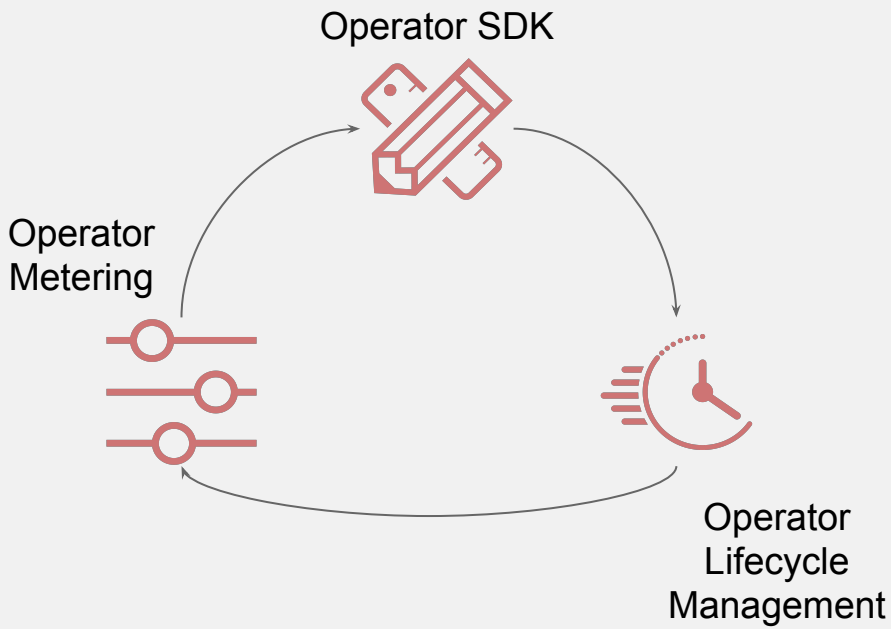
```
> odo create wildfly backend
Component 'backend' was created.
To push source code to the component run 'odo push'

> odo push
Pushing changes to component: backend

> odo storage create backend-store --path /data --size 100M
Added storage backend-store to backend

> odo create php frontend
Component 'frontend' was created.
To push source code to the component run 'odo push'

> odo push
Pushing changes to component: frontend

> odo url create
frontend - http://frontend-myproject.192.168.99.100.nip.io

> odo watch
Waiting for something to change in /Users/tomas/odo/frontend
```

Developer Productivity with OpenShift

Eclipse Che	VSCode	CDK & minishift	OpenShift.io
Beta of Red Hat supported Che on OpenShift by end of CY18 Red Hat supported SKU (pricing TBD) bundled with OpenShift	OpenShift connectivity plugin Istio & Knative schema for content assist Iterative dev	Continue alignment with OCP install options (operators) Addon support for Istio and Knative Alignment with minikube	Add support for deploying apps and components to OpenShift Dedicated Eval MW: Fuse and AMQ Simplified UX flows

Operators

OPERATOR FRAMEWORK



OPERATOR FRAMEWORK

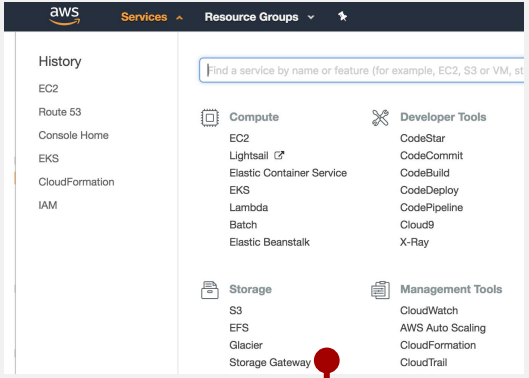
Operator Framework is an open source toolkit to manage application instances on Kubernetes in an effective, automated and scalable way.

Operators = Automated like the cloud

AVAILABLE NOW

Your app...

automated like the cloud...



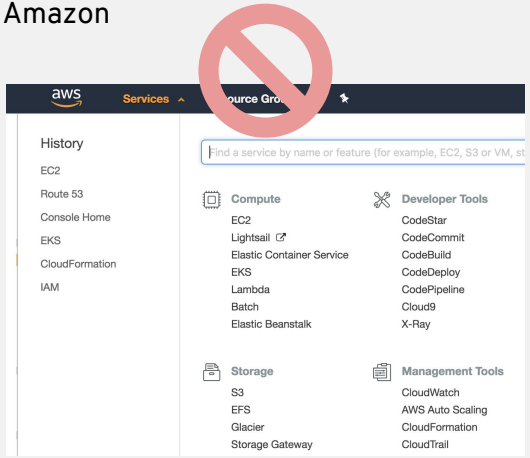
but runs on...

Operators = Native Kubernetes experience

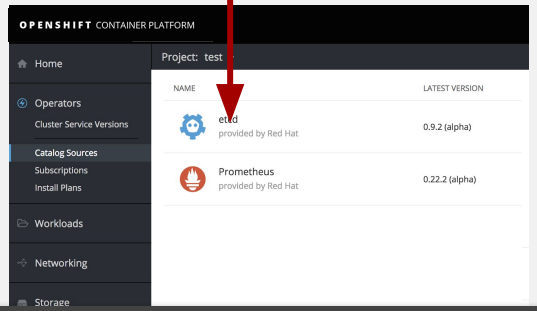
AVAILABLE NOW

Your app...

Can’t register your internal service with Amazon



Can have native support in OpenShift, including the CLI

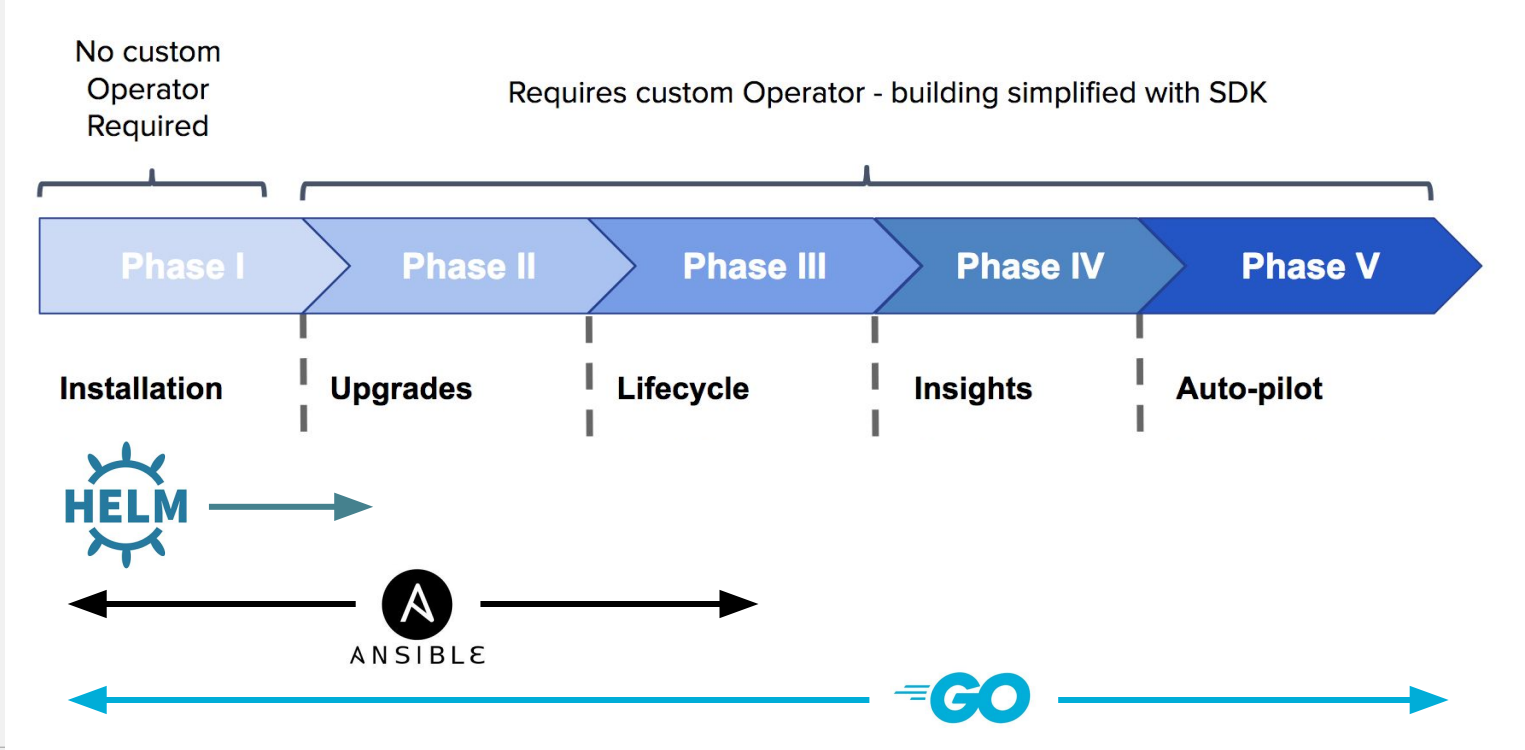



```
$ oc get mongodbs
$ oc scale --replicas=3 mongodb/example
```


redhat.

Operator Maturity Model

HELM & GO AVAILABLE NOW
ANSIBLE Q1 2019

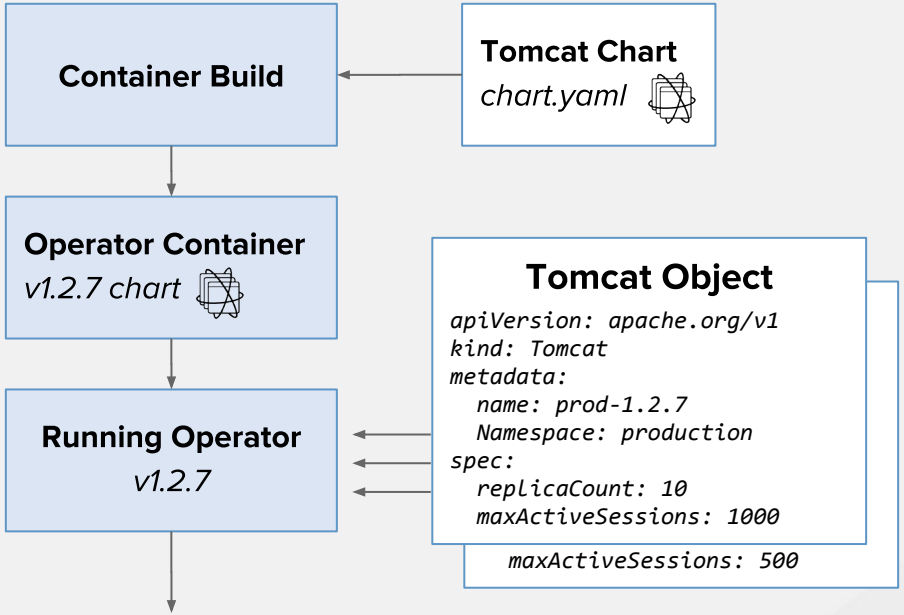


Helm Operator with existing charts

AVAILABLE NOW

- Supported model for running Helm charts
- Build an Operator with no code written
- Immutable artifact/container for each released version
- More secure
  - No tiller running
  - Operator calls Helm internal code a library
  - Builds on existing cluster RBAC

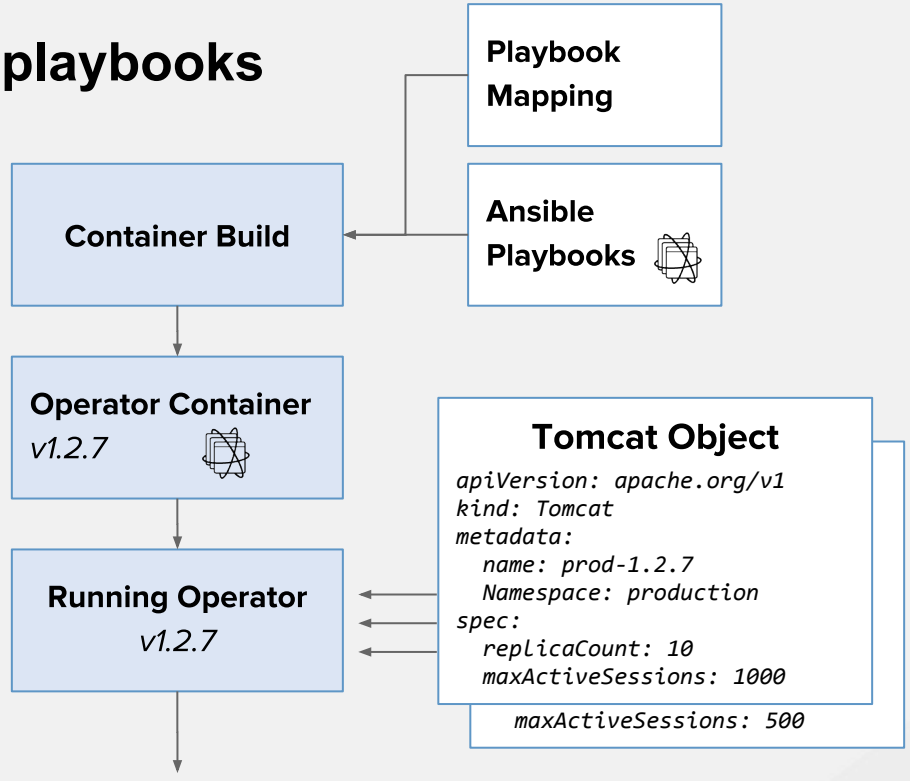
[Read the blog post]




```
$ oc get Tomcats --all-namespaces
NAMESPACE     NAME            READY    STATUS    RESTARTS   AGE
production    prod-1.2.7      1/1      Running   0          4d
staging       staging-v1.2.8  1/1      Running   1          2h
```

Ansible Operator with existing playbooks

- Supported model for running Playbooks in an Operator fashion
- Great for Ops teams that aren't traditional devs
- Takes the human out of the loop
- Connects the playbooks to Kubernetes events like Node failures



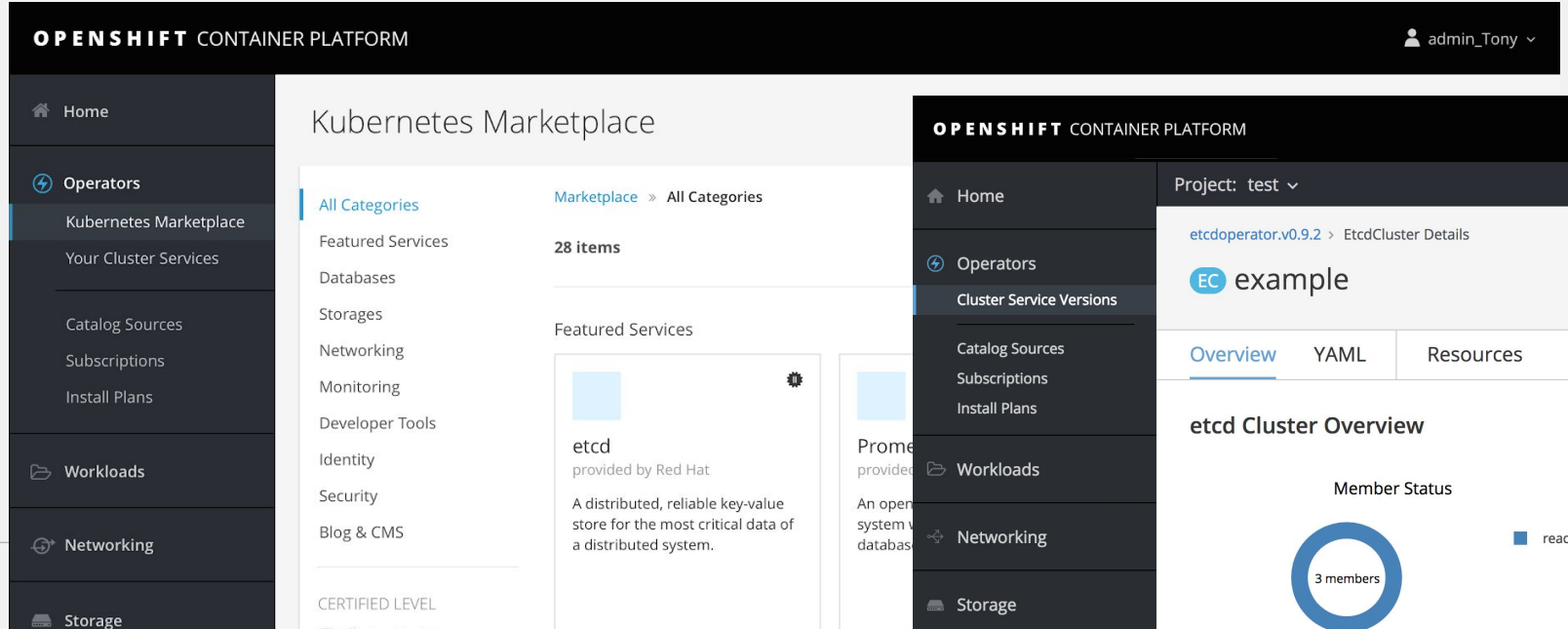

```
$ oc get Tomcats --all-namespaces
NAMESPACE     NAME             READY     STATUS    RESTARTS   AGE
production    prod-1.2.7       1/1       Running   0          4d
staging       staging-v1.2.8   1/1       Running   1          2h
```

AVAILABLE 3-6 MONTHS

Operators = Integration for Red Hat products & ISVs

TARGET FOR 4.0

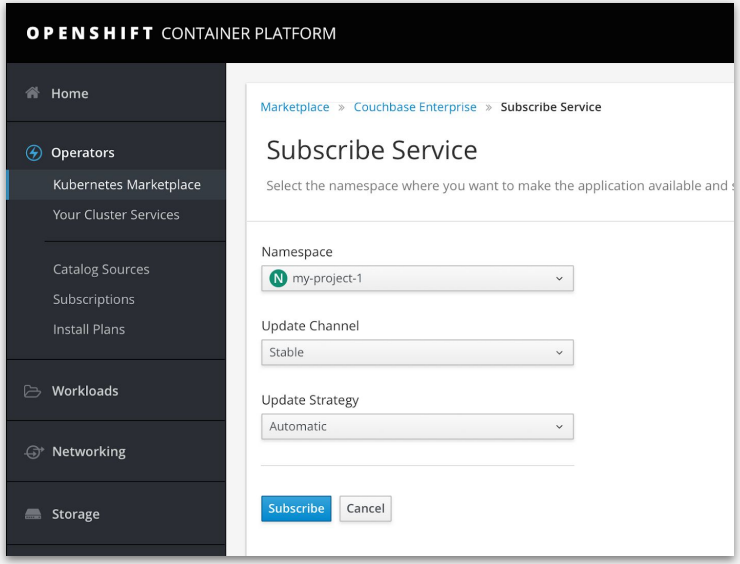
- Marketplace for discovering Fuse, AMQ Streams, Container Storage, Container Native Virtualization
- Graphical integration with the Console & Operator Lifecycle Manager

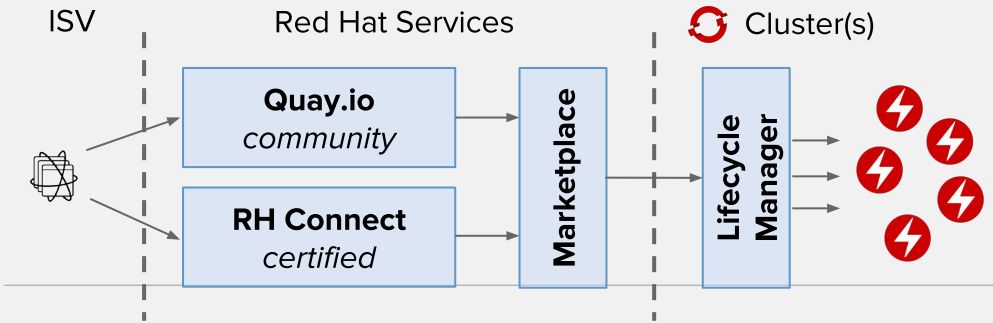


Lifecycle Manager + Marketplace power over-the-air updates for apps

TECH PREVIEW 3.11
GA 4.0

- Allow product teams to ship outside of OCP releases
- Self-service for customer eng. teams
- Doesn't require user to have admin access to install CRDs
- Marketplace is backed by Quay.io
- Offline will be powered by Quay Enterprise

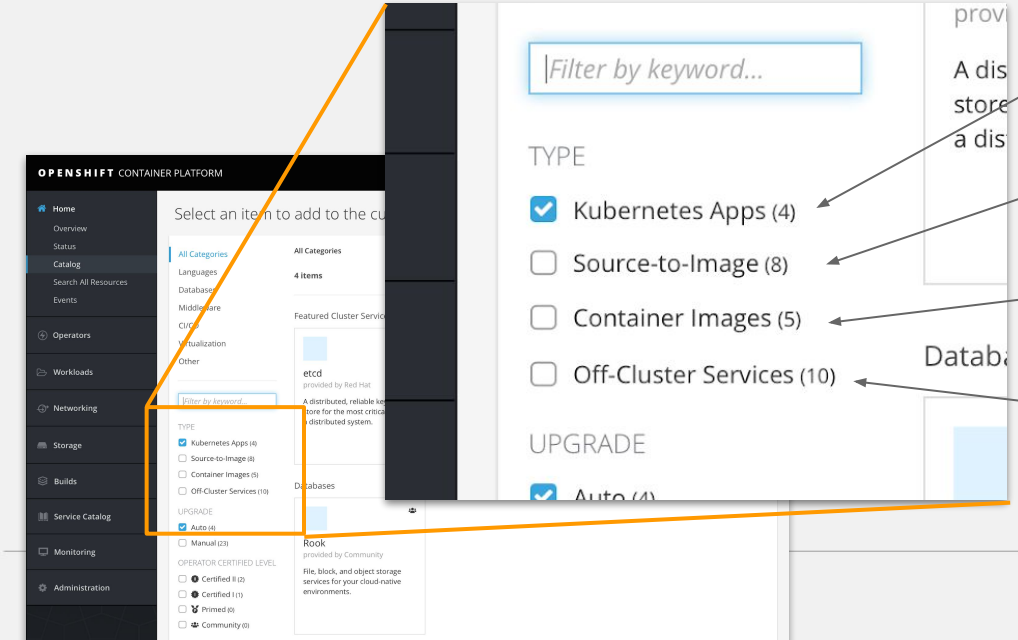




Redesigned Catalog brings it all together

TARGET FOR 4.0

- Better communication about how to use specific entries
- Highlight Red Hat products and runtimes
- Plan for Cloud Brokers installed by default



Operator Catalog ← OPERATOR SDK: Go, Ansible, Helm

Source 2 Image ← Existing RH content; Customer s2i

Ansible Broker & others ← Existing content

Cloud Brokers ← Azure; aws

Service Catalog & Brokers

Service Catalog - What's Next

Injection of Binding Data

Objective: reduce manual steps

After a service is provisioned, and bound, a `secret` is created

`secret` will be added to a deployment configuration using `PodPreset`

Deployment Config Change trigger will cause redeployment of pods, which will include binding data.

Service Governance

Objective: allow fine-grained control on who can provision and bind to services.

Scenario: in my organization developers can only provision and bind to development services. Production apps have access to services tagged as production-ready and are controlled by a different group

OpenShift Automation Broker - What's Next

Developer Enhancements

Ability to preserve state during different method calls.

Working with a shared remote cluster

- Better certificate handling with APB tool
- Support workflows with s2i and Broker discovery of built image
- Leverage Namespaced ClusterServiceClasses to allow a developer to publish APBs for testing that they can see but are not cluster wide

Better sanity checks, early warnings in

- Add sanity checks for APB spec and syntax to APB tool, currently tool does little to no checks and relies on Broker/ServiceCatalog to detect errors
- Improve Broker to validate all specs prior to sending to Service Catalog

Ansible Galaxy Integration

Publishing APB's to Ansible Galaxy using the ansible-galaxy tooling.

Automation Broker will discover those published APBs to Ansible Galaxy, download, and run them in source form.

Greatly enhances developer experience when using OpenShift and Ansible together. Allows developers to search Galaxy and leverage content for example APBs and benefit from the APB specification now being a supported format for Galaxy content.

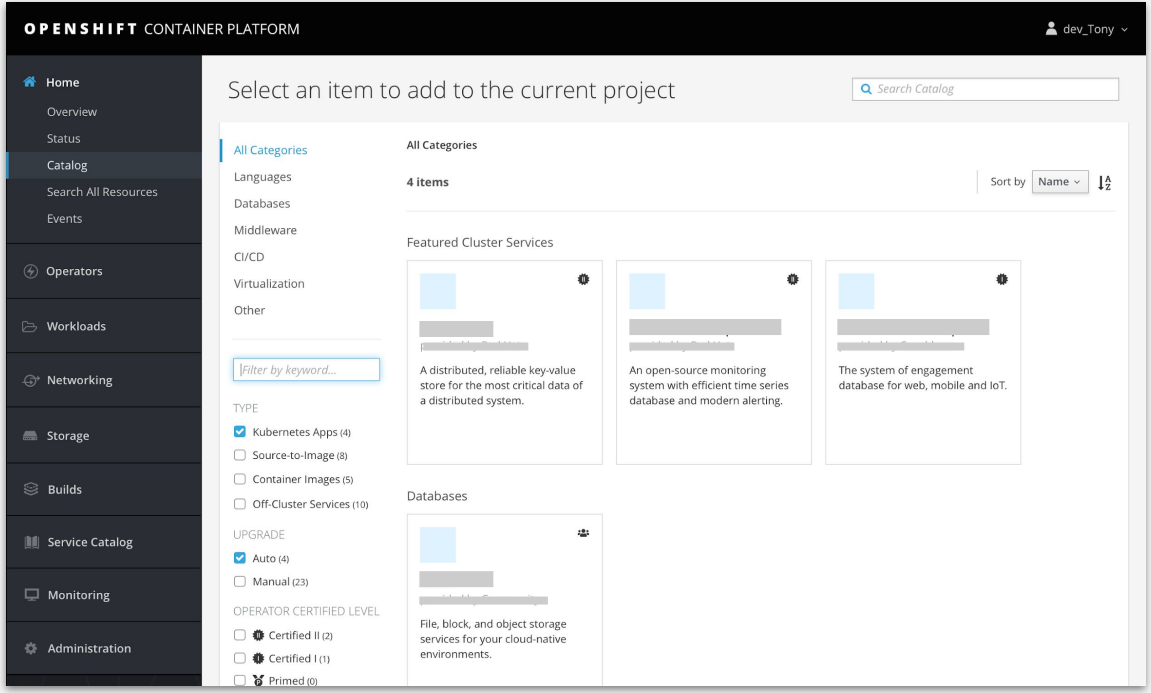
- Consuming Ansible Galaxy Roles using an APB

GALAXY

aws
Service Broker

AWS Service Broker

AMAZON WEB SERVICES



New AWS Services:

- **Kinesis Data Streams**
- **Key Management Service (KMS)**
- **Lex**
- **Polly**
- **Rekognition**
- **Translate** *(requires Preview registration)*
- **SageMaker**

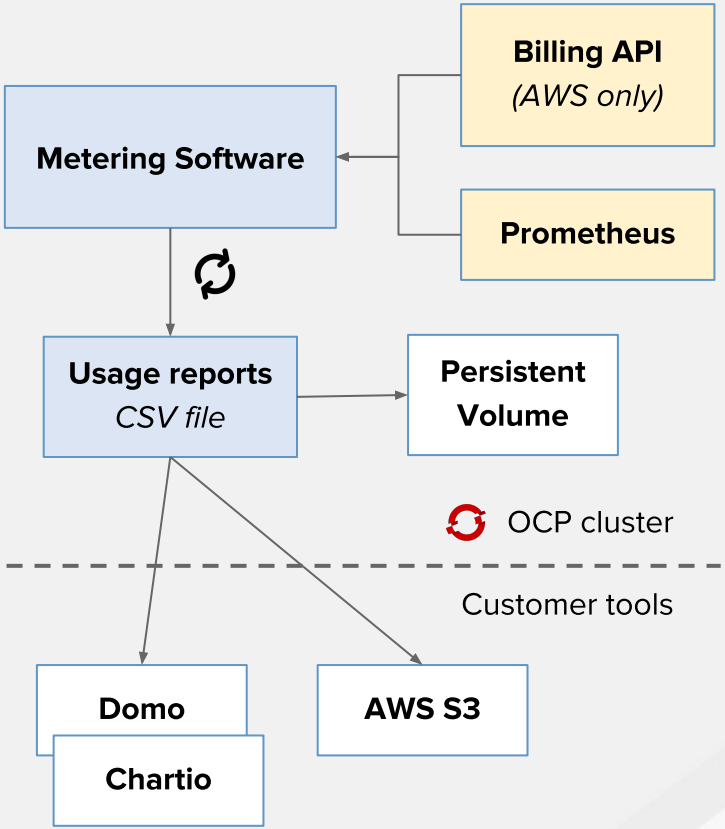
Additional RDS engines:

Aurora, MariaDB, and **PostgreSQL**

Management & Metering

Metering (Chargeback)

- Consumes data from cluster's Prometheus
- Periodic reports
  - Requested resources or usage based
  - Reports per pod, node or namespace
  - AWS only: calculate $$ amount for reports
- Only tracks CPU, RAM to start
- Basis for future consumption based pricing
- Offer basic UI reporting but main use is to plug into customer's BI tool of choice

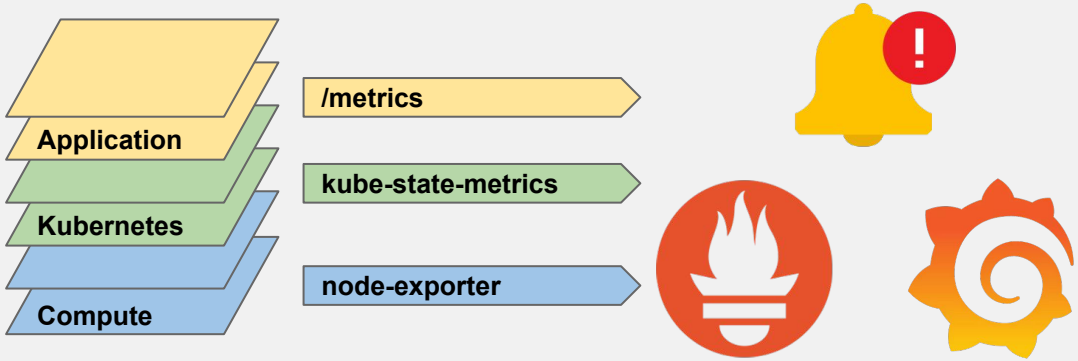


Prometheus Cluster Monitoring GA

3.11

Feature(s):

- Query and plot cluster metrics collected by Prometheus.
- Receive notifications from pre-packaged alerts, enabling owners to take corrective actions and start troubleshooting problems.
- View pre-packaged Grafana dashboards for etcd, cluster state, and many other aspects of cluster health.



See what alerting rules and metrics are included, as well as other information about the OpenShift Cluster Monitoring stack:

Unified, native cluster-level Alerting UI

3-6 months

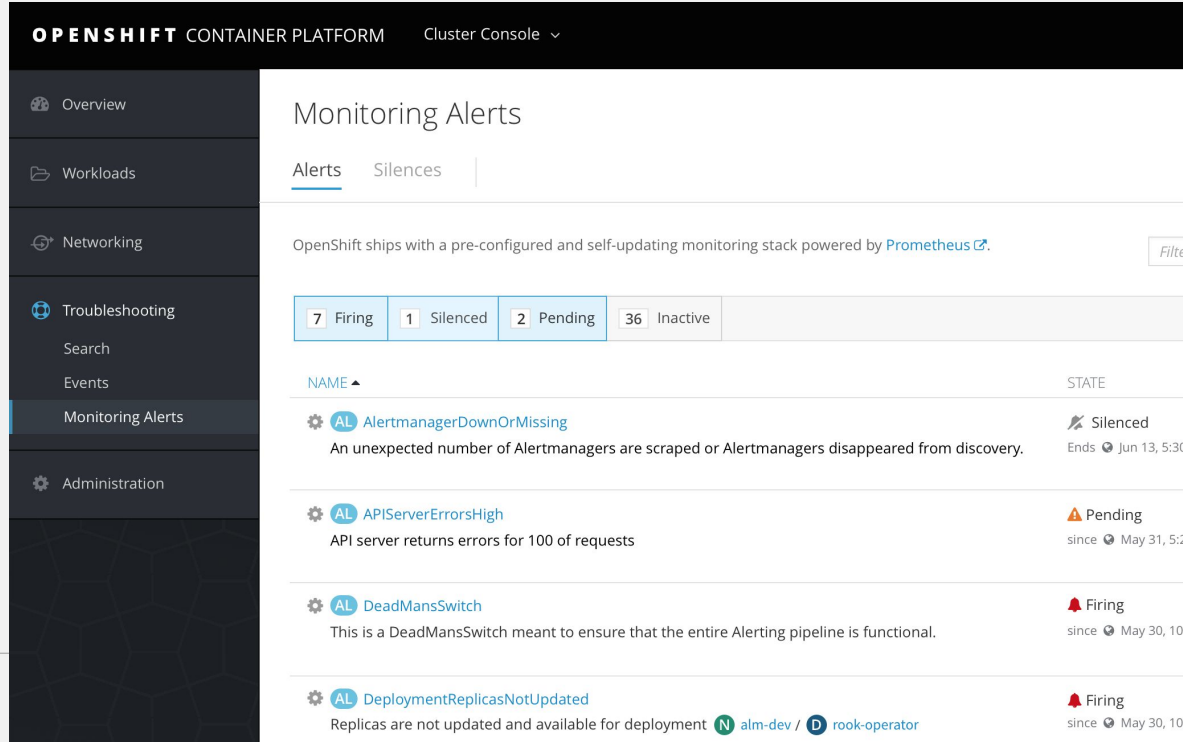
Objective: Provide a single, unified, and native experience for Cluster Admins to manage alerts and start troubleshooting.

Feature(s):

- Manage all your alerts in one place.
- Understand details of an alert and start troubleshooting.
- Silence specific groups of alerts.
- Configure notification systems through the UI.

Future (subject to change):

- Connect Alerts with Logs/Metrics and quickly browse data more quickly to find the cause of a problem



Prometheus as a Service through the Operator Catalog

3-6 months

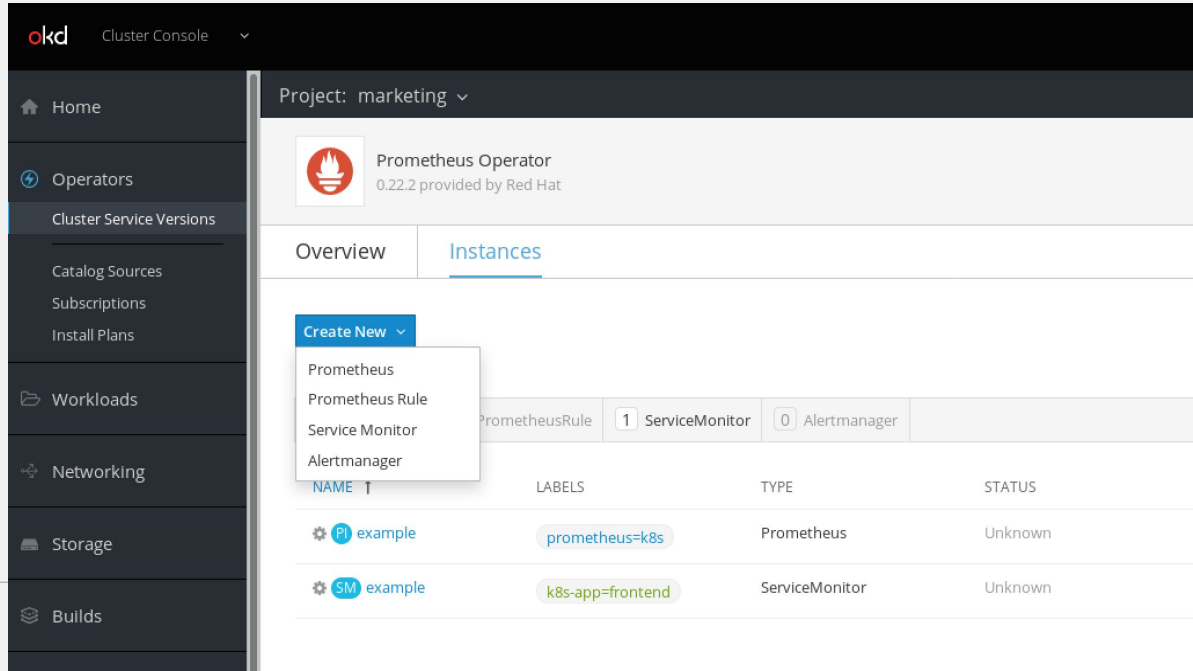
Objective: Provide a streamlined experience to setup app monitoring with Prometheus for tenants through the Operator Catalog.

Feature(s):

- Easily manage all your Prometheus/ Alertmanager instances in one place
- Simplified configuration
- Let project admins deploy their own monitoring stack.

Future (subject to change):

- Automatically deploy entire stack to monitor apps
- Adding Grafana



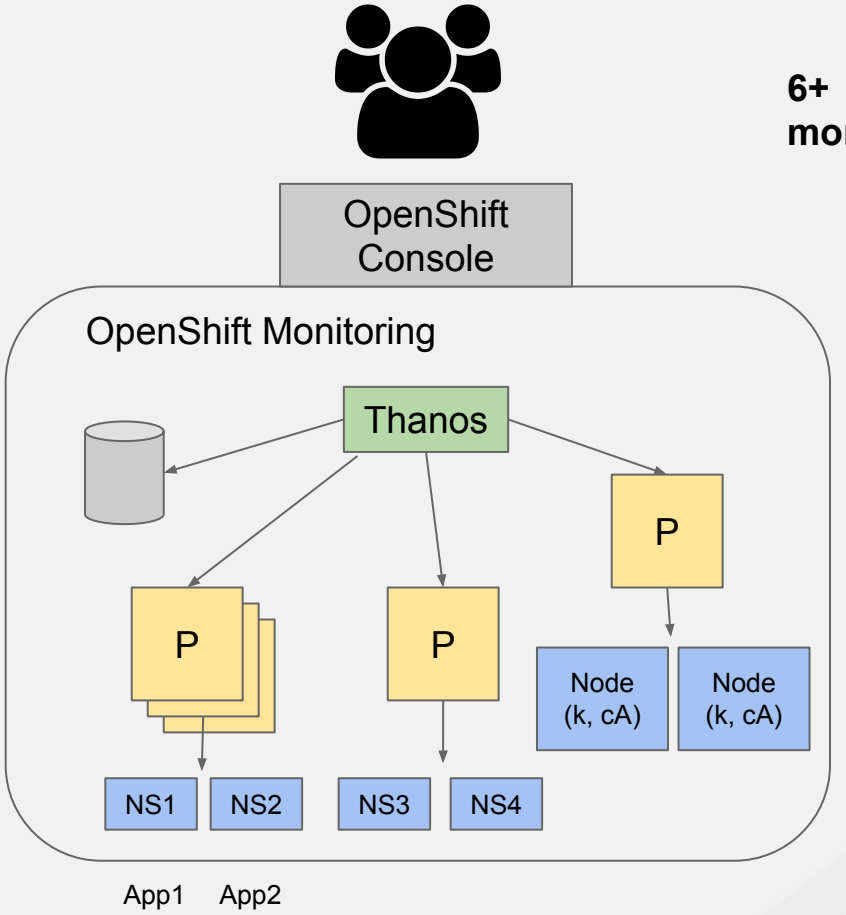
Introducing Thanos

Objective: Productize Thanos to support critical customer use cases.

Feature(s):

- Long-term storage.
- Global querying view across all connected Prometheus servers.
- Downsampling, allowing you to query years of data.

Currently under investigations.



6+ months

Monitoring/ Metrics - Summary

Next 3 months

Query and plot cluster metrics

Get notified and take corrective actions

View various infra-related dashboards with Grafana

3 - 6 months

View and react to alerts natively in OpenShift

Configure monitoring your apps through OLM

More than 6 months

Long-term storage for metrics

Connect metrics and log data to decrease MTTR

Add customer specific dashboards and rules for cluster-level monitoring

Growing the number of alerting rules & Grafana dashboards we ship with OpenShift

Improving troubleshooting experience through native, holistic insights across all telemetry data

Logging

OCP 3.11

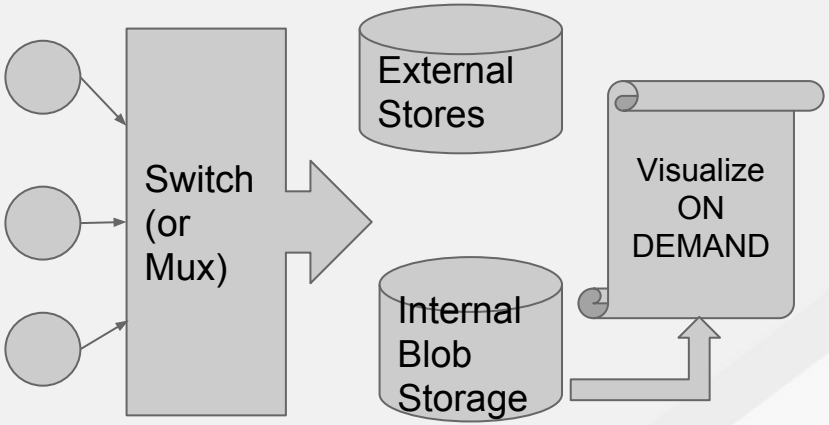
- ES 5.x “stack” GA

Future

- Logging operator(s)
- Prometheus monitoring of Logging
- Alerting on Logs/events
- Rsyslog for log collection
- Logging to Kafka
- On demand Logging

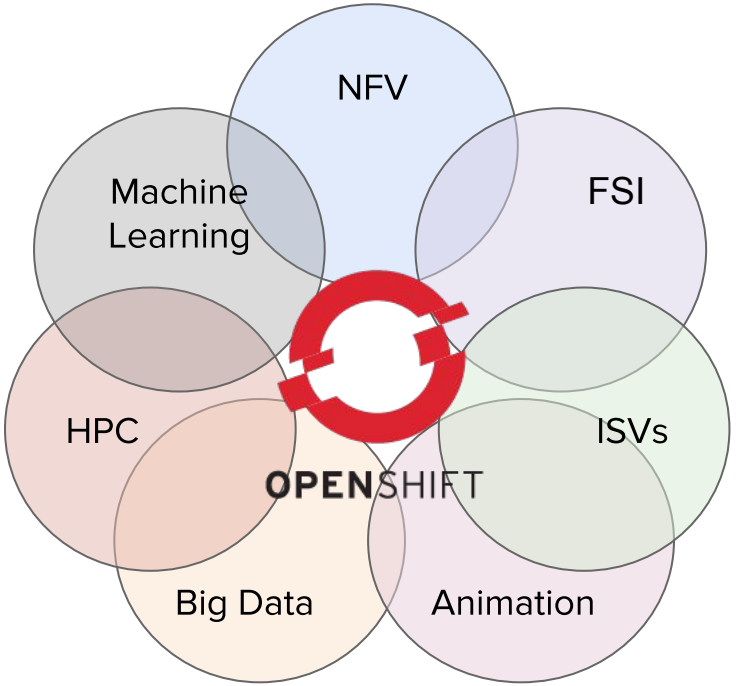
ON DEMAND LOGGING

- Majority of collected log data is not used
- Indexing unused log data is expensive
- On-demand access to log data



P-SAP

Performance Sensitive Applications (P-SAP)



GPU support in OpenShift

Current (3.10)

- Device Manager GA
- HowTo enable Nvidia GPUs on OpenShift

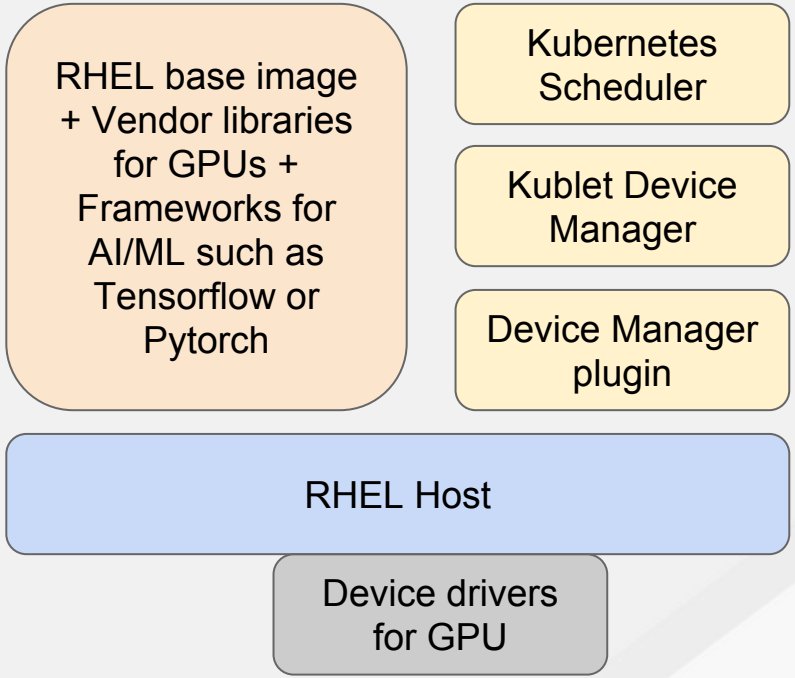
Next

- Reference Architectures
- Certifications and support
- Seamless install experience

Beyond

- Nvidia container images in RHCC Registry
- GPU Monitoring
- Specify GPU resource at a granular level

```
kind: Pod:
    resources:
      limits:
        nvidia.com/gpu: 1
#requesting 1 GPU
```



P-SAP Plans

Current (3.10)

- CPU Manager, Hugepages

Next

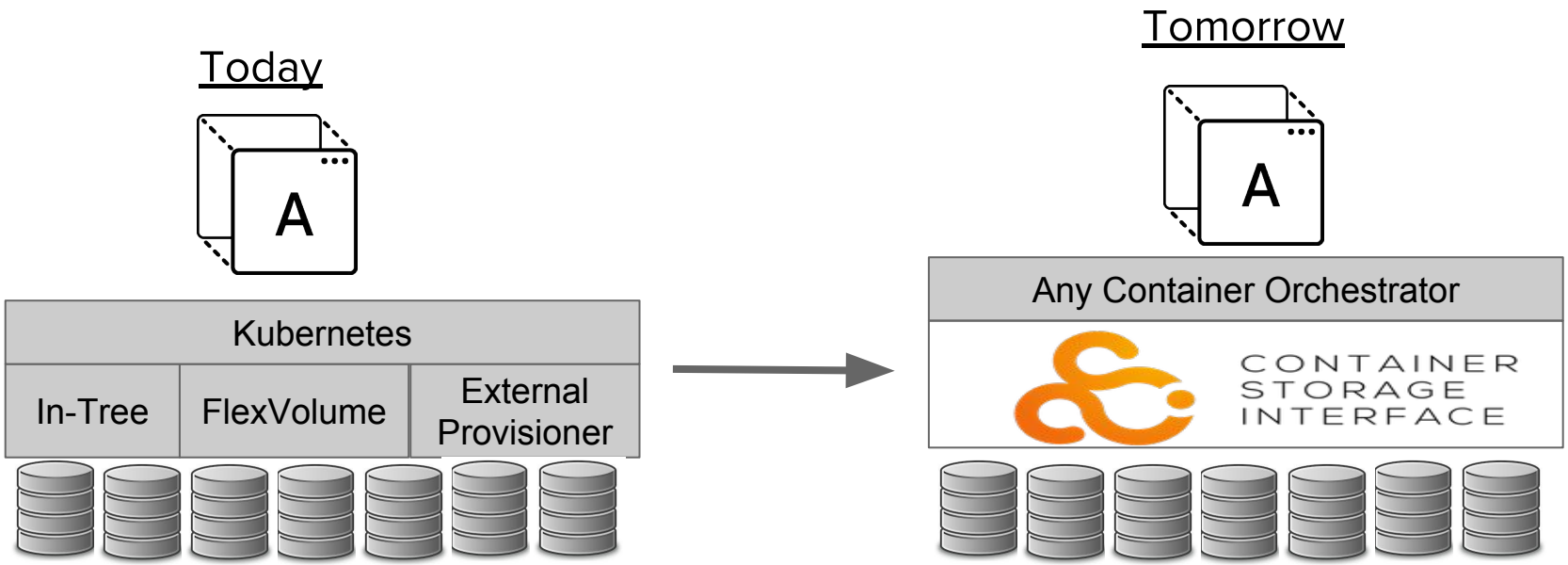
- Node Tuning Operator

Beyond

- Numa Awareness
- Scale operator

Storage

Storage Projects



Transitioning from Tech Preview to GA

- Local PersistentVolumes
- Raw Block Volumes
- Volume Snapshot and Restore

New Exciting Projects in 2018:

- Storage operators
- CSI GA
- CSI Ember plugin

redhat.

OpenShift Container Storage

OCS 3.10
Sep 18

- Arbiter Volume Support
- Block backed PV stability
- Enhanced OCS metrics

OCS 3.11

- Vol Resize w/ Web Console
- Install Pre & post checks

OCS 4.0/4.1

- Operator for install & upgrade
- Heketi functionality merge with GCS
- Intg monitoring using Prometheus/Grafana
- Integrated Management using Tectonic Console
- RHOCS object stack
- CSI , Snapshot, Clone
- Service Broker/Catalog integration

Istio

Istio

- Connect
- Secure
- Control
- Observe

Istio - Cloud Native Service Mesh

Connect

Control the flow of traffic between services:

- A/B Testing
- Quantile based deployments
  - Canary Deployments
  - Staged Rollouts
- Fault injection
- Traffic mirroring

Secure

Application independent security:

- Zero trust network
- Mutual Transport Layer Security (TLS)
  - Service to service encryption
- Service to service authentication
  - Transport authentication
  - Origin authentication

Istio - Cloud Native Service Mesh

Control

Uniform abstraction for policy control

- Allow for traffic redirection in response to real time events
  - Response codes
  - Service latency
- Rule based processing based on headers

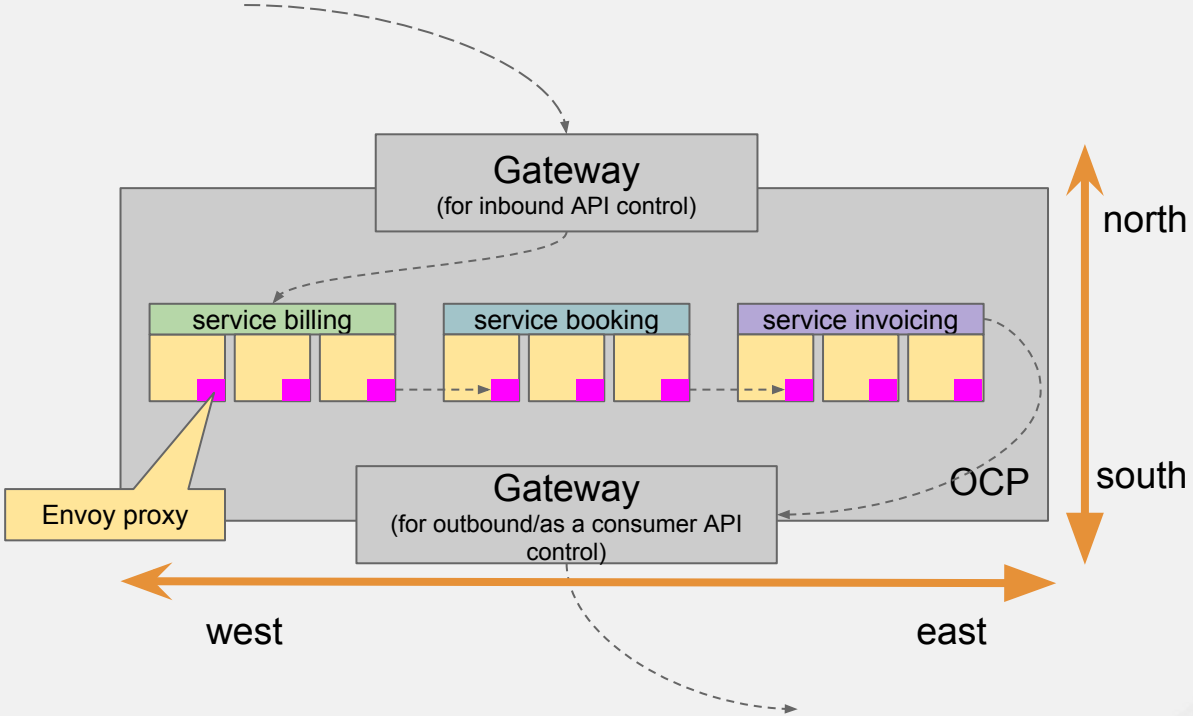
Observe

Visibility into application deployments

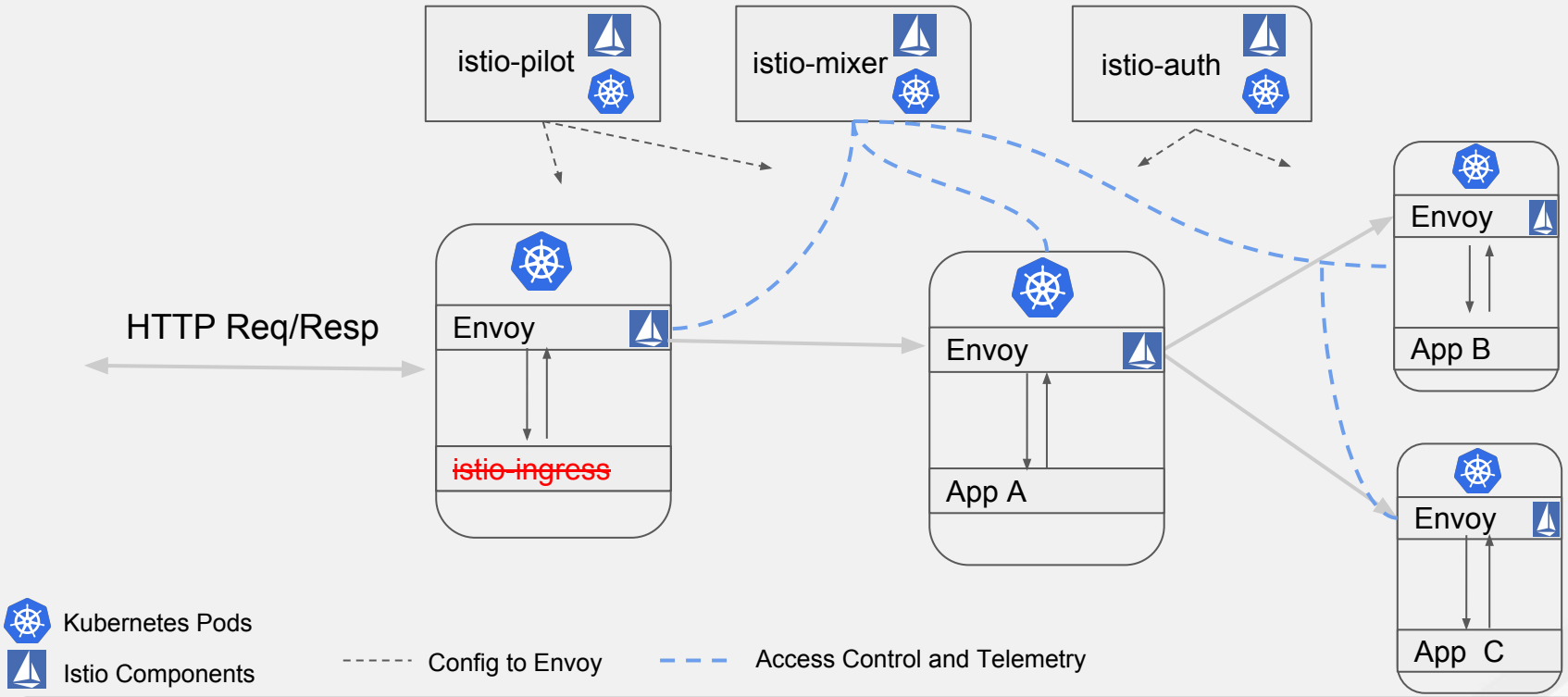
- Pluggable backend for telemetry capture
  - Allows for COTS applications to get non-zero visibility into performance
  - Prometheus
  - Others TBD based on customer need
- Application tracing
  - Jaeger
- Service topology
  - Kiali

Istio

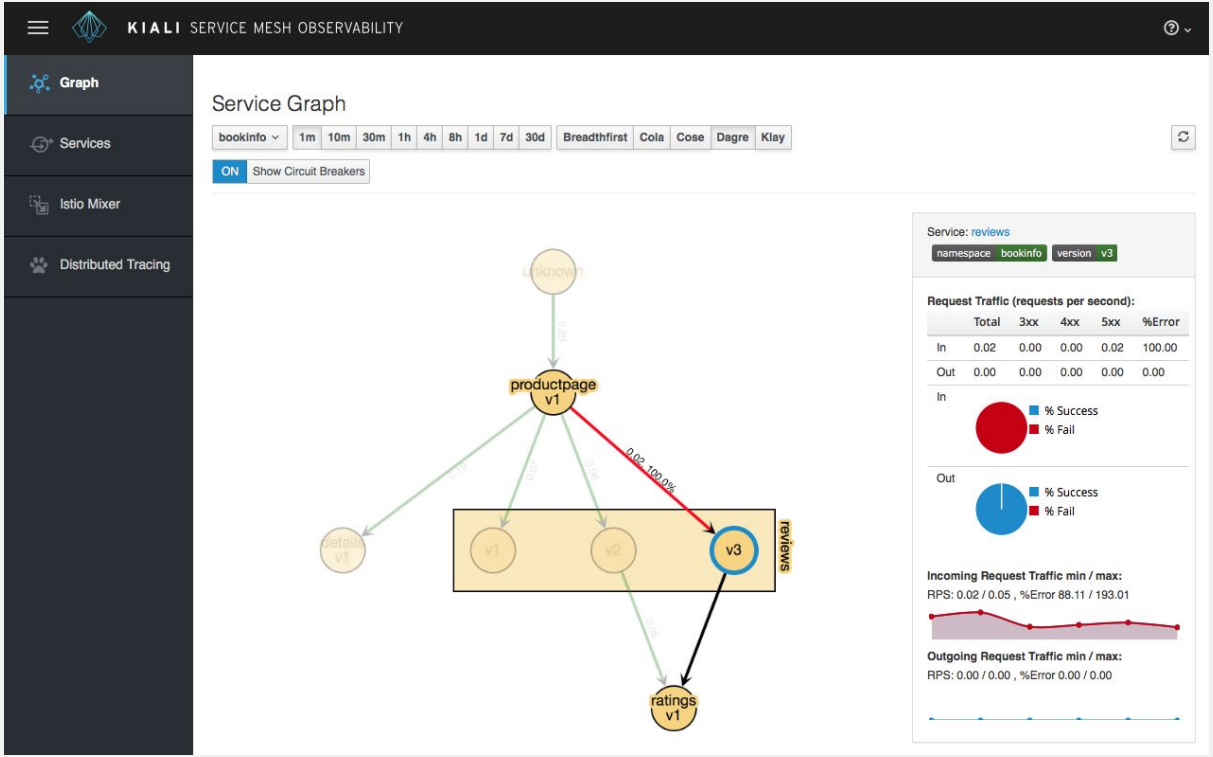
- **Intelligent Routing and Load Balancing**
- **Resilience Across Languages and Platforms**
- **Telemetry and Reporting**
- **Policy Enforcement**



Istio Service Mesh



Istio (& Kiali)


KIALI SERVICE MESH OBSERVABILITY
Graph
Services
Istio Mixer
Distributed Tracing
Service Graph
bookinfo
1m 10m 30m 1h 4h 8h 1d 7d 30d
Breadthfirst Cola Cose Dagre Klay
ON Show Circuit Breakers
Unknown
productpage v1
details v1
v1
v2
v3
reviews
ratings v1
0.02, 100.0%
Service: reviews
namespace bookinfo
version v3
Request Traffic (requests per second):
Total 3xx 4xx 5xx %Error
In 0.02 0.00 0.00 0.02 100.00
Out 0.00 0.00 0.00 0.00 0.00
In
% Success
% Fail
Out
% Success
% Fail
Incoming Request Traffic min / max:
RPS: 0.02 / 0.05 , %Error 88.11 / 193.01
Outgoing Request Traffic min / max:
RPS: 0.00 / 0.00 , %Error 0.00 / 0.00

Istio - What's different?

Istio is an "operator first product" (using Operator Framework)-
https://github.com/Maistra/istio-operator

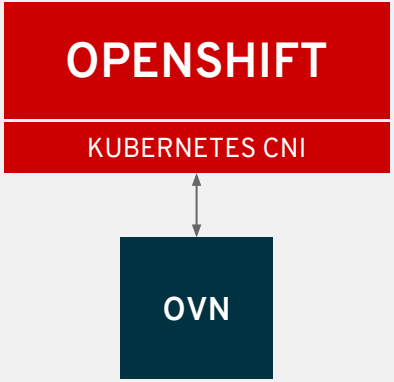
The operator manages the install. In the future it will manage updates as well.

Istio is delivered as *containers,* **not** RPMs

Tech Preview starts 2018-09-04 with install docs in the OpenShift Container Platform & Origin docs (look under "service mesh install")

Advanced Networking

Open Virtual Network (OVN)



Next-Gen Default OpenShift SDN

- An implementation of virtual networking via Open vSwitch project
- Developer Community
  - SDN portfolio consolidation / common network tech (RH-OCP, RH-OSP, RHV)
- Acceleration and enablement of customer-driven feature requirements
  - Egress IP per pod
  - Distributed Ingress/Egress firewall
  - Distributed services LB
  - Multi-Network/Interface
  - Heterogeneous clusters w/ Windows nodes
  - Capability to span on-prem & cloud nodes
  - Traffic isolation / Multi-tenancy
  - DPDK support
  - Encrypted tunnels
  - IPv6 / DHCPv6
  - QoS, Control/Data plane separation
  - ...

OVN Enablement Timeline

OCP 3.9/3.10

- “Developer Preview” for clusters with Windows servers

OCP 3.11

- “Developer Preview” for clusters with Windows servers

OCP 4.0

- Tech Preview for all OCP clusters

OCP 4.1

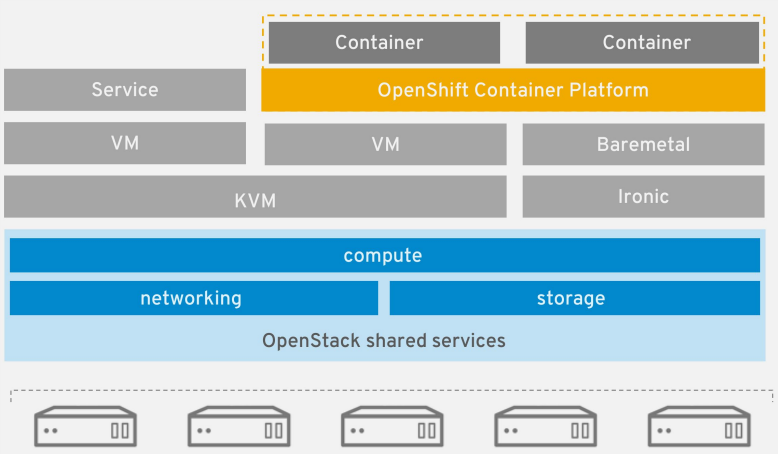
- OVN GA
- Default SDN

Improved OpenShift Integration with RH-OSP

Project goal: **Provide best practice out-of-the-box OCP+OSP integration**

- Remove double-encapsulation issue
- Direct use of rich shared services provided by the underlying OSP cloud:
  - LBaaS, FWaaS, DNSaaS, …
  - Immediate compliance with Neutron plugins

- OSP's tenant isolation becomes directly effective on OpenShift, as well
- Bare metal provisioning and management via Ironic

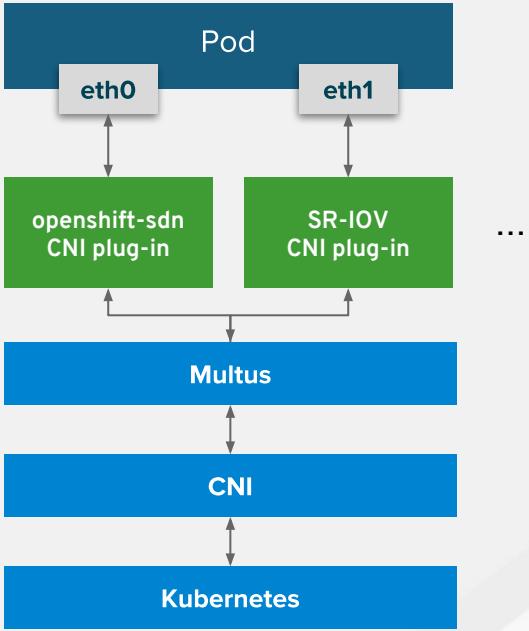


Enabling technology: Kuryr

Multus

- Problem: Kubernetes only supports one network interface, “eth0”, but we need:
  - Functional separation of control/data planes
  - Link aggregation for network redundancy
  - Different network protocol stacks, capabilities, SLAs
  - Traffic isolation / Network segregation and security
  - QoS
- Solution: Multus “meta plug-in” for Kubernetes CNI
- Enables multiple network interfaces per pod, each assigned a different CNI plug-in defined in pod spec
  - Each with its configuration defined in CRD objects
- SR-IOV enablement

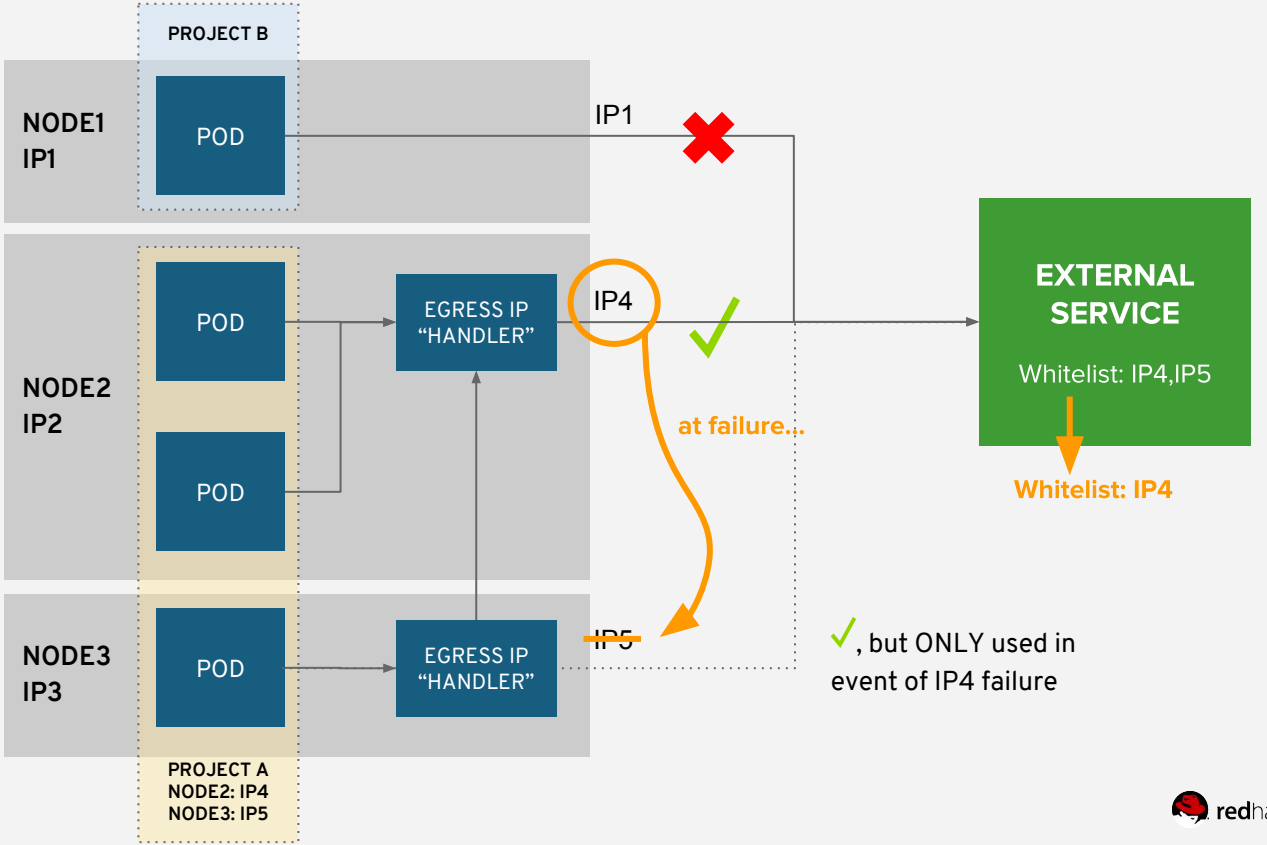
Pod with Multus



Fully Automatic, HA Namespace-Wide Egress IP

Enhance our current (3.10.1) HA egress source IP solution to allow for migration of a single egress IP address.

= future work



redhat.

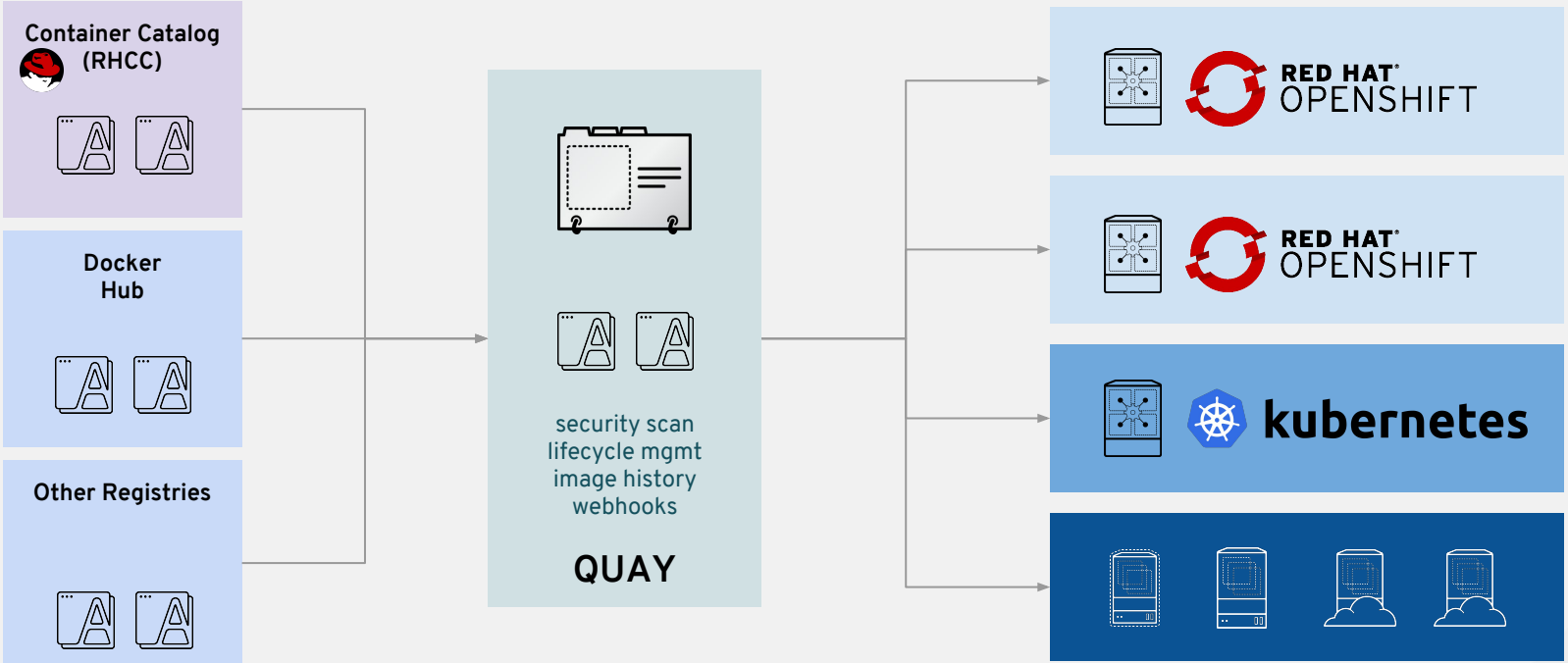
Networking Enhancements

- Enhance Kubernetes NetworkPolicy support
  - egress
  - ipBlock
- Operators are in-progress for improved installation, scaling and upgrades:
  - OpenShift SDN
  - OVN
  - kuryr-kubernetes (in conjunction with OSP DFG)
  - ODL (in conjunction with CTO group)
  - 3rd-Party SDN guidance documentation

```
...
egress:
  - to:
    - ipBlock:
        cidr: 10.0.0.0/24
    ports:
    - protocol: TCP
      port: 5978
...
```

Registry

Content Ingress with Quay



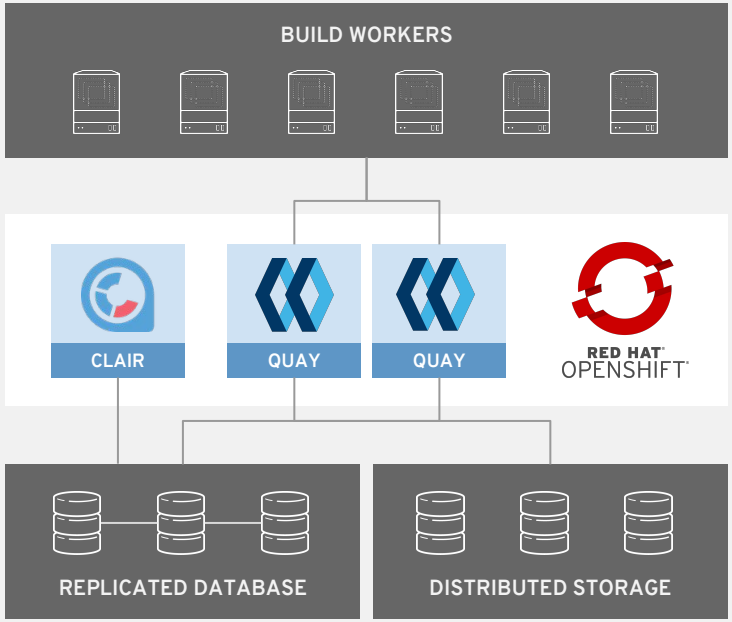
Quay on OpenShift: Recommended Setup

On OpenShift Cluster:

- Quay Enterprise
- Clair

Outside OpenShift cluster:

- Database
- Storage
- Builders



Quay Roadmap Planning

Until e/o CY 2018

- OCI distribution spec v2_2
- Red Hat Quay v3
- Clair v3
- Documentation updates
- Open sourcing Quay
- App centric UI (marketplace)

CY 2019

- Repository mirroring
- Deeper integration into OCP
- Signing enhancements
- “Quay everywhere”

Future Features Further Details

- Red Hat Quay v3 (targeted for Oct 2018)
  - Red Hat Quay images now based on RHEL base images
  - Rebranding of UI and Logo to ensure consistent UX with other RH products
  - OCI distribution spec v2_2
    - Required for Multi-Arch and to store other blobs inside the registry (operator)
- Quay Operator support (phased deliverables, initial support Nov '18)
  - Ability to store and maintain operators including the operator manifest
  - Full UI and API support for operator based applications

Future Features Further Details

- Open sourcing Quay (targeted for mid of Dec'18, KubeCon)
  - Making source code available and submit to CNCF
- Clair v3
  - Redesign of Clair to support both OS level and programming language package managers in parallel (currently either or)
  - Still leveraging OVAL streams for RH content with all its limitations, other metadata sources such as NVD used as well though
  - long term planning: full RH content coverage, Container Health Index and 3rd party scanning support

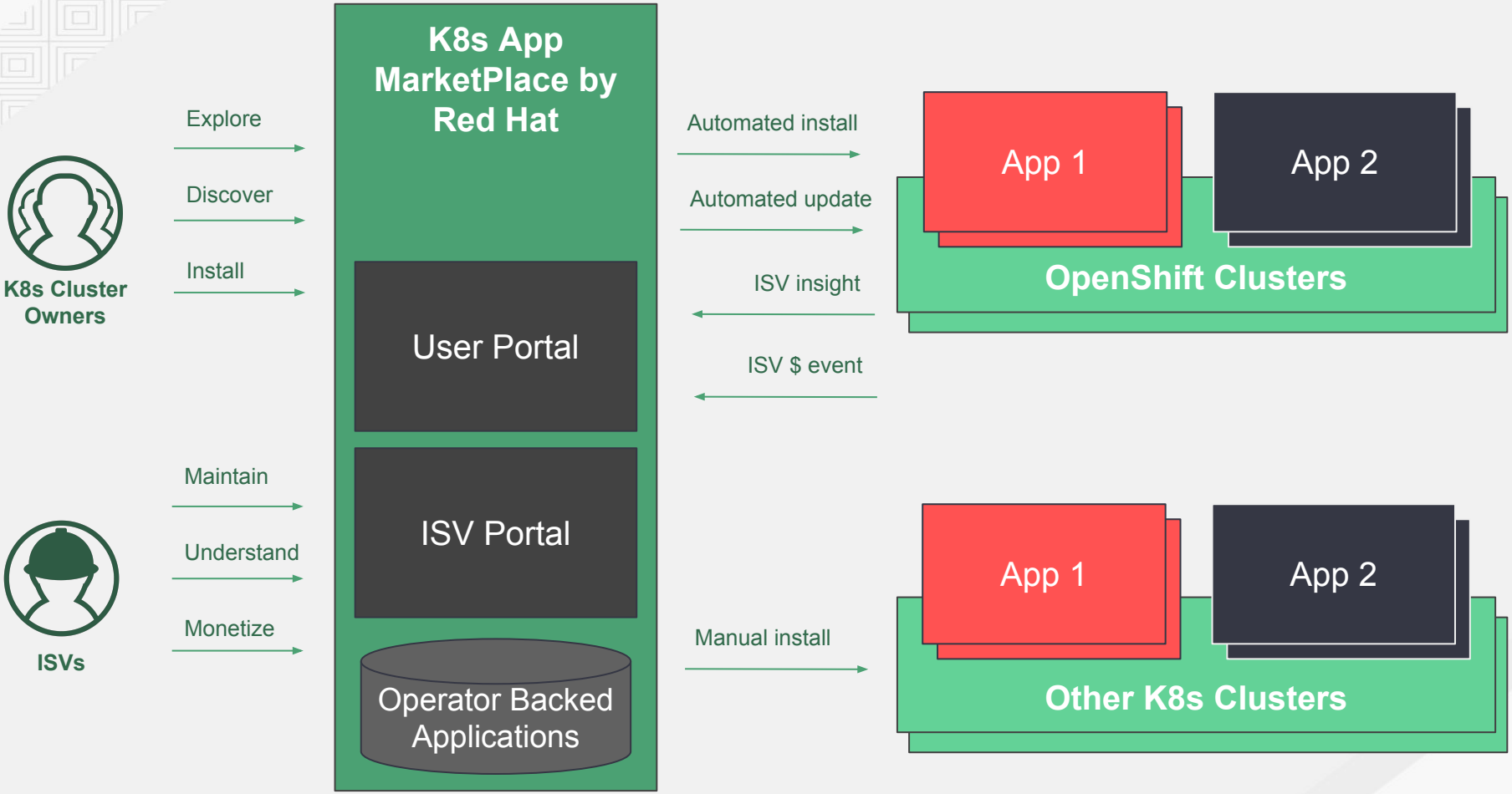
Future Features Further Details

- Application centric UI (Marketplace) targeted for Summit '19
  - Enhancing the application registry features currently limited to Helm charts to support operators including content sourcing and distribution and governance
  - Marketplace UI available in 3 different flavors (see next slides)
- Deeper integration into OpenShift (targeted for Q3CY2019)
  - better integration and UX fit customers using both OpenShift and Quay
  - Includes data, events, users and RBAC, field input appreciated
  - Note: Quay can be used with OCP already today as any other ext registry
  - S2i and Imagestream updates are currently not supported yet

Future Feature: Repository Mirroring

- Currently planned for early CY 2019
- High priority feature requested by many customers
- Allows ongoing mirroring of external repositories into Quay
  - Including filtering by tags / versions
  - Includes non-image repositories (operators)
- Future extensions:
  - Better offline support
- Temporary workaround: skopeo copy

Operator Distribution & Marketplace


K8s App MarketPlace by Red Hat
K8s Cluster Owners
Explore
Discover
Install
User Portal
ISVs
Maintain
Understand
Monetize
ISV Portal
Operator Backed Applications
Automated install
Automated update
ISV insight
ISV $ event
App 1
App 2
OpenShift Clusters
Manual install
App 1
App 2
Other K8s Clusters

KUBERNETES APPLICATION MARKETPLACE

PHASED DEVELOPMENT

Phase 1
Operators Packaged with OpenShift
- 4-5 ISV Operators

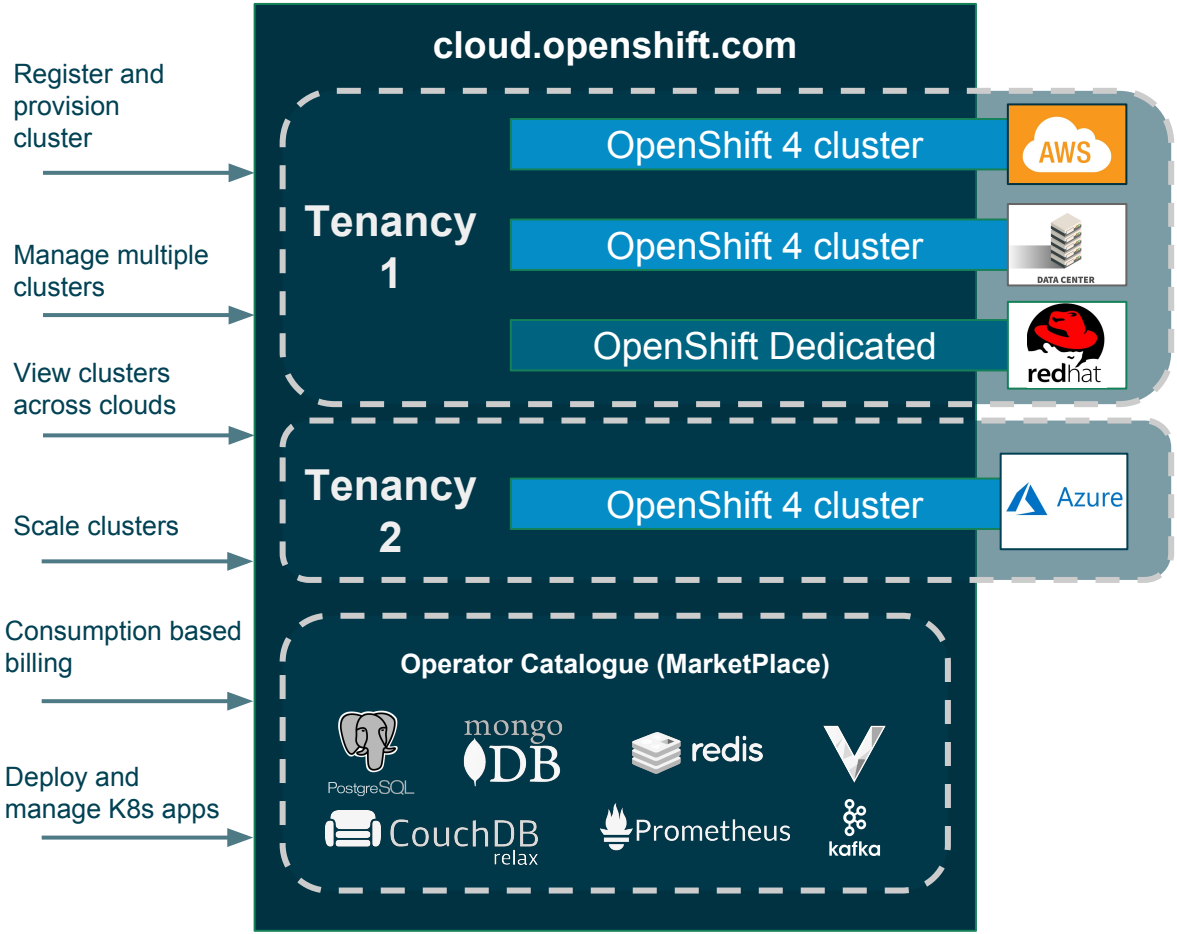
Phase 2
Marketplace local to cluster
Sync Operators from Quay - ~20
Certified Operators

Phase 3
Public Marketplace - 100's of
community and certified operators

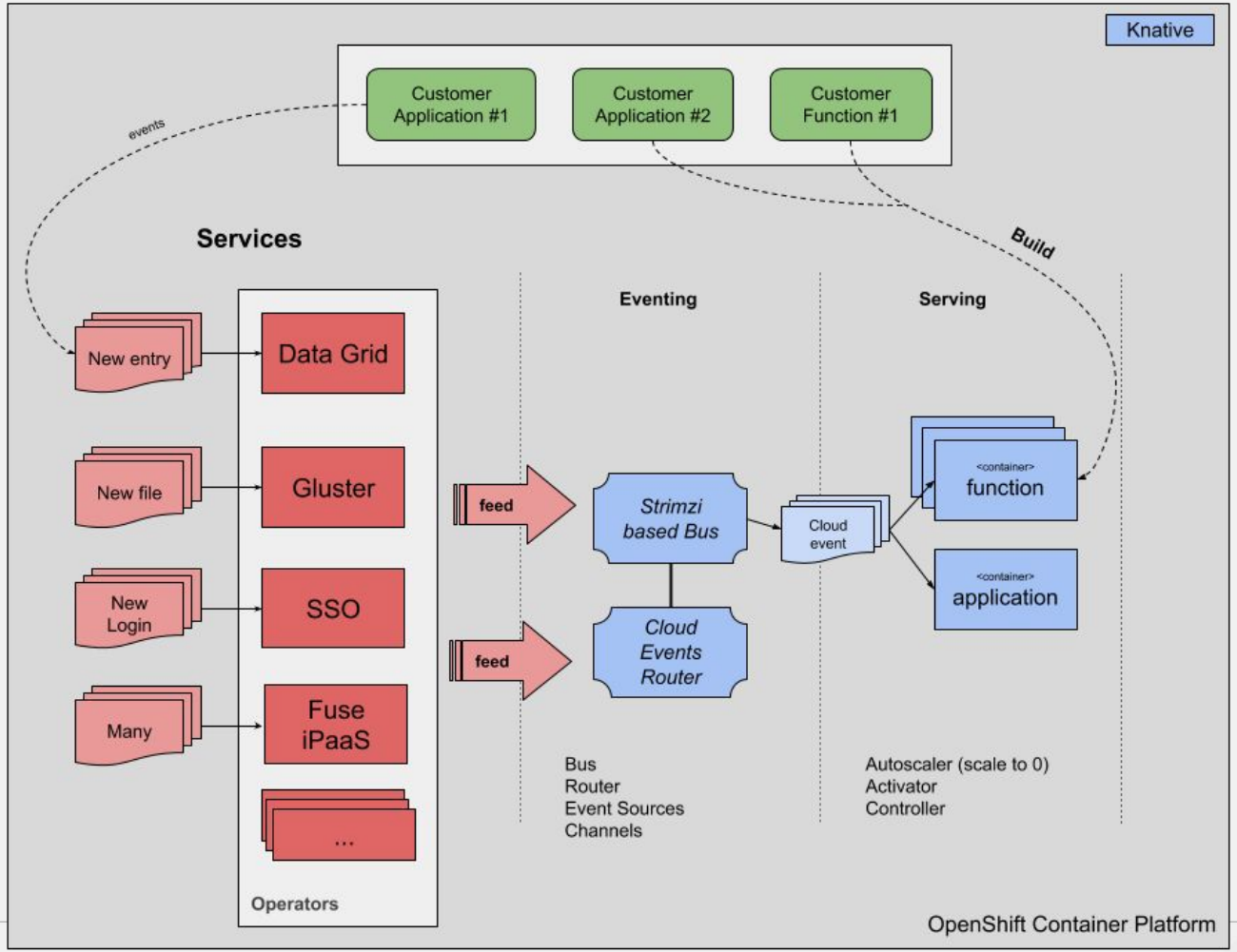
Unified Hybrid Cloud

Unified Hybrid Cloud

- Manage clusters across all infrastructure - On-prem or across cloud providers
- Deploy true hybrid services - behave like a cloud with full portability
- Pay based on consumption - with option to separate cloud bill
- Optionally choose fully managed (dedicated)



KNative


Knative
Customer Application #1
Customer Application #2
Customer Function #1
events
Build
Services
New entry
New file
New Login
Many
Data Grid
Gluster
SSO
Fuse iPaaS
...
Operators
Eventing
Serving
feed
feed
Strimzi based Bus
Cloud Events Router
Cloud event
<container> function
<container> application
Bus
Router
Event Sources
Channels
Autoscaler (scale to 0)
Activator
Controller
OpenShift Container Platform

Security

AUTOMATED & INTEGRATED SECURITY

CONTROL
Application Security

- Container Content
- CI/CD Pipeline
- Container Registry
- Deployment Policies

DEFEND
Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

EXTEND

- Security Ecosystem

Authentication & Authorization

Next 3 months

- Support Windows Kerberos as Identity Provider (Tech Preview)
- Github Enterprise as Identity provider
- KeyStone IP enhancements: Synchronize projects & related role-bindings

3 - 6 months

Integration with external KeyCloak for advanced token management (Dev preview) -- as an alternative to OpenShift OAuth solution

Consume group memberships from an external Identity Provider

More than 6 months

Integration with external KeyCloak (Tech Preview)

Certificate & Secrets Management

Next 3 months

Notify of expiring certs during upgrade

3 - 6 months

Operator to install, configure and manage the certificate signing server

*PEM files become secrets and behave like any other secret on the platform***

More than 6 months

Improve certificate management with ACME server proxy & client plugins

KSM integration via Citadel

Hardening & Compliance

Next 3 months

Openshift to CIS Kubernetes benchmark mapping spreadsheet

FISMA Moderate, ISO27001 PAGs

PCI-DSS Reference Architecture

Add forbiddenSysctls and allowedUnsafeSysctls options to SCCs

3 - 6 months

OpenShift built with FIPS compliant golang (*dev preview)* *

- only available with RHEL in FIPS mode

More than 6 months

User namespace support

Migrate SCC → Pod Security Policy

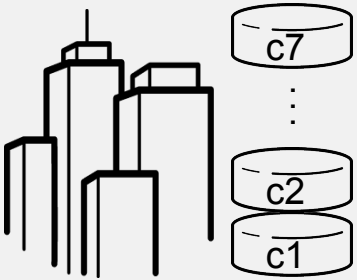
OpenShift built with FIPS compliant golang (GA)

- Only available with RHEL in FIPS mode
- CRI-O required

*FIPS Certification of OpenShift: **Targeted for CY 2019.** Our RHEL 7.6 FIPS evaluation, currently underway, includes use cases of OpenShift running on RHEL 7.6 patched with the Golang libraries which call RHEL-provided crypto (e.g. OpenSSL). **This configuration has not been tested by QE**.

Federation

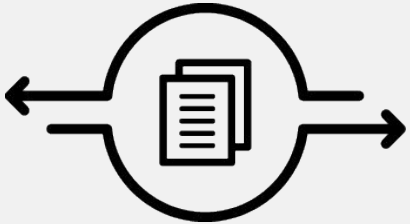
Federation V2 - Multi-Cluster Service Delivery



OpenShift Clusters c1 through c7

$ openshift-install launch

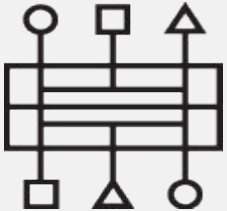
Cluster Registry Operator



Single Source of Truth

$ oc get clusters

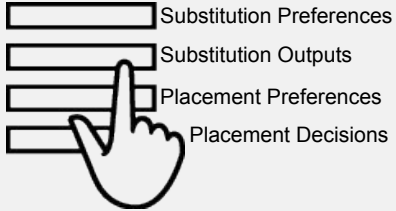
Federated API Operator



Base Federated Resources

FederatedDeployment
FederatedSecret
FederatedReplicaSet
FederatedConfigMap

Schedule and Reconcile



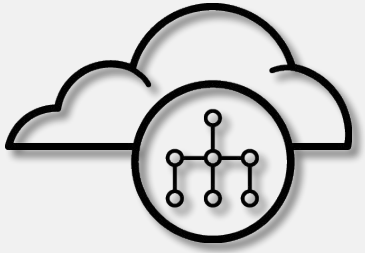
Auxiliary Resources

```
overrides:
  clusters:
  - clusterName: c1
    replicas: 5
  - clusterName: c3
    replicas: 10
  - clusterName: c7
    replicas: 15
```

https://github.com/kubernetes/community/tree/master/sig-multicluster

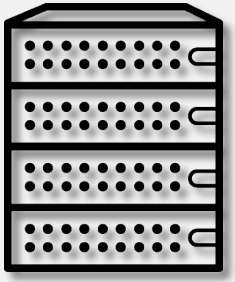
Install & Upgrades

OpenShift 4 Installation Experiences



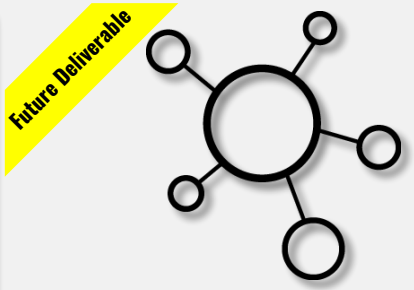
OPENSHIFT by Red Hat + CoreOS

Next Gen Installer
Opinionated “Best Practices”
single cluster provisioning



OPENSHIFT by Red Hat + RED HAT ENTERPRISE LINUX

Node Customization
RHEL host based
single cluster provisioning



OPENSHIFT by Red Hat → OPENSHIFT by Red Hat

OpenShift Hive
Multi-cluster provisioning
& orchestration

4.0 Beta Jan '19

Next Gen Installer

Opinionated “best practices” single cluster provisioning

- CLI-based installer designed to easily provision a “best practices” OpenShift cluster on RH CoreOS infrastructure
  - 4.0: AWS, OSP
  - 4.1: Azure, Bare Metal
  - 4.2: VMware, GCP
- Guided workflow allowing users to walk through each step and customize as needed:
  - `init → render → prepare → launch`
- Only supports deployments on immutable infrastructure (RH CoreOS)
  - Host OS updates are fully automated and pushed alongside OpenShift updates
- Quickly download installation client (with embedded token) from cloud.openshift.com and run from anywhere (Linux, Windows, and Mac) to deploy OpenShift
- New installs only; no in-place upgrade support for OCP 3.11

```
# Generate initial installation configuration
$ openshift-install init
    Select a supported provider [aws/azure/openstack]: aws
    Enter the base-domain: foo.example.com

Generated ./install-config.yaml

# Modify config settings (e.g EC2 master machine sizes)
$ vi ./install-config.yaml

# Render assets from install-config parameters
$ openshift-install render

# Edit rendered assets (e.g modify kube-dns manifest)
$ vi ./manifests/kube-dns-daemonset.yaml

# Generate final assets for use in bootstrap tool (ignition,
tfvars)
$ openshift-install prepare
$ git add . && commit -m ‘my cluster’

# Launch from generated assets:
$ openshift-install launch
```

Node Customization

RHEL host based single cluster provisioning

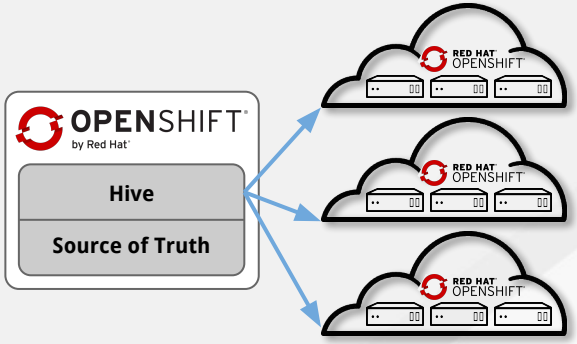
- Traditional method for installing OpenShift clusters, but with significant refactoring in 4.0
  - Focus will only be on new cluster installations
  - Cluster upgrades will now be performed from the cluster console with the operator framework
  - Minimizes openshift-ansible's role to just the initial configuration needed for provisioning a control plane, top level operator, and compute nodes
- Easily provision OCP 4.0 on nodes running on-premise or in the public cloud
  - 4.0: RHEL
  - 4.1: RH CoreOS (beta in 4.0)
- Allows existing node provisioning tooling to be leveraged by customers
  - Customers can customize RHEL based on their environment requirements
  - RHEL OS updates are the responsibility of the administrator, but to assist with this a playbook will be provided with hooks to facilitate a rolling restart of the nodes after upgrading the OS
- Support for in-place upgrades of OCP 3.11 (RHEL-based) clusters to OCP 4
  - Specific OCP versions for upgrade path to be determined
  - Won't support moving off RHEL nodes to immutable RH CoreOS nodes
  - Won't support OCP 3 + RHEL Atomic upgrades; customers must first move to RHEL before upgrading

Future Deliverable

OpenShift Hive

Multi-cluster Provisioning & Orchestration

- Reliably provision/deprovision, upgrade, & configure OpenShift (& RH CoreOS) clusters
  - 4.0: Limited Developer focused release
    - Support for installing/uninstalling on AWS only; upgrades won't be supported in initial release
    - Enables developers to easily stand up real-world clusters for development and testing of various OpenShift components (operators, core kube, etc)
    - Same system can be used to drive automated CI/CD testing of PRs
- Installed on OpenShift cluster via an operator
  - Becomes central source of truth for all clusters it manages
- Leverages work from:
  - ***Next gen installer*** - Uses CLI to launch clusters in the public cloud
  - ***Unified Cluster API*** - Declarative, Kubernetes-style API for cluster creation, configuration, and management



https://github.com/openshift/hive

Install, Upgrade, & Migration Paths to OpenShift 4

New Installation Paths

amazon web services | RED HAT OPENSTACK PLATFORM | Microsoft Azure | RED HAT ENTERPRISE VIRTUALIZATION | Google Cloud Platform | vmware vSphere

Public & Private Cloud

Node customization with RHEL hosts

+ RED HAT ENTERPRISE LINUX 7.x / 8.0 → INSTALL → OPENSHIFT by Red Hat 4.0 + RED HAT ENTERPRISE LINUX 7.x / 8.0 Beta

amazon web services | RED HAT OPENSTACK PLATFORM

Public & Private Cloud

Next gen installer (openshift-install) → INSTALL → OPENSHIFT by Red Hat 4.0 + CoreOS

OpenShift 3.11 Upgrade Path

OPENSHIFT by Red Hat 3.11 + RED HAT ENTERPRISE LINUX 7.x** → UPGRADE → OPENSHIFT by Red Hat 4.0 + RED HAT ENTERPRISE LINUX 7.x

AWS / OSP Only!

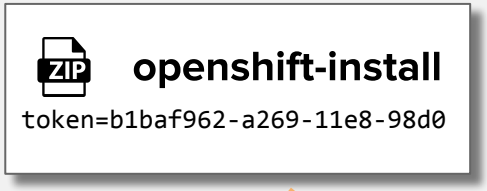
If running on AWS or OSP, RHEL 7 nodes can be replaced with RH CoreOS for compute and infrastructure nodes only → CoreOS

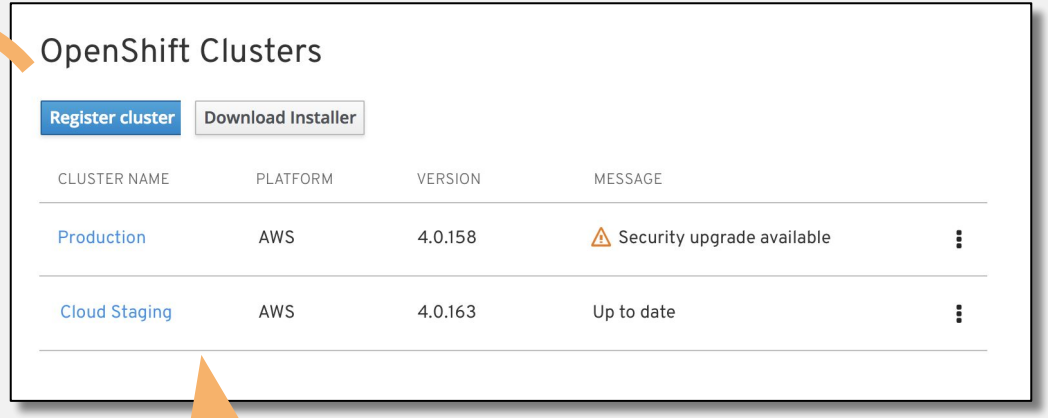
Tectonic 1.9 Migration Path

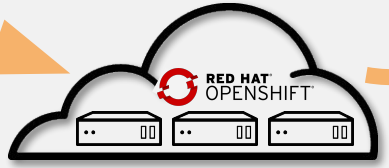
TECTONIC by CoreOS 1.9 + container linux → WORKLOAD MIGRATION → OPENSHIFT by Red Hat 4.0 + CoreOS

*** No in-place upgrade support planned for RHEL Atomic*

Unified Hybrid Cloud & Over-The-Air Updates

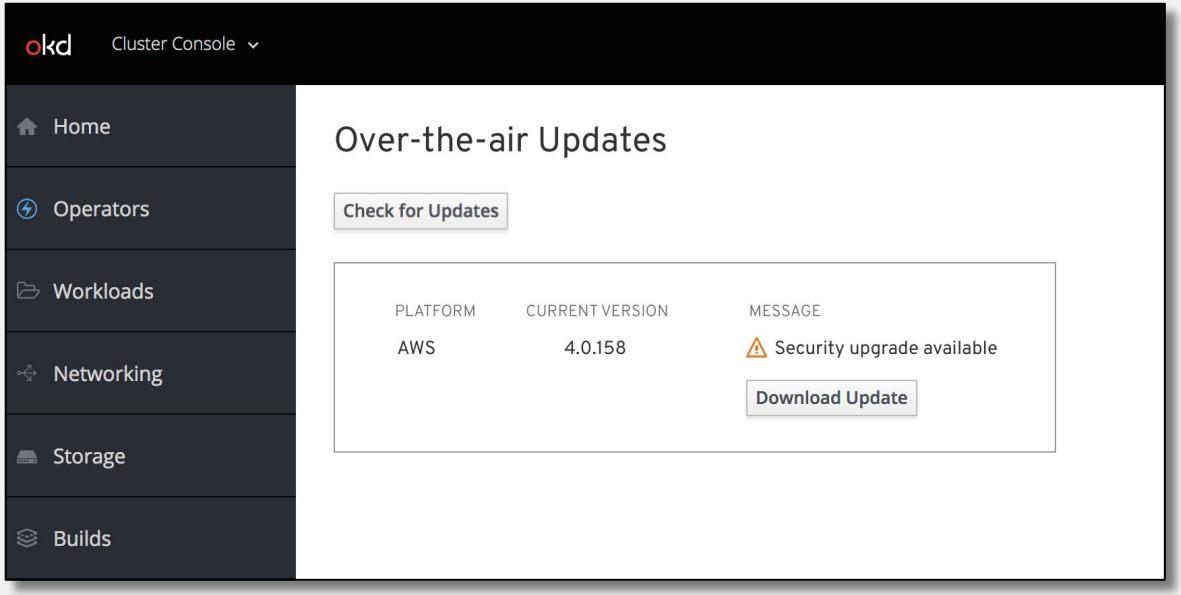






- New installer with embedded token will be available for download from cloud.openshift.com
- Clusters will get registered in *cloud.openshift.com*
- View/control over-the-air updates across all clusters

On-Premises Updates

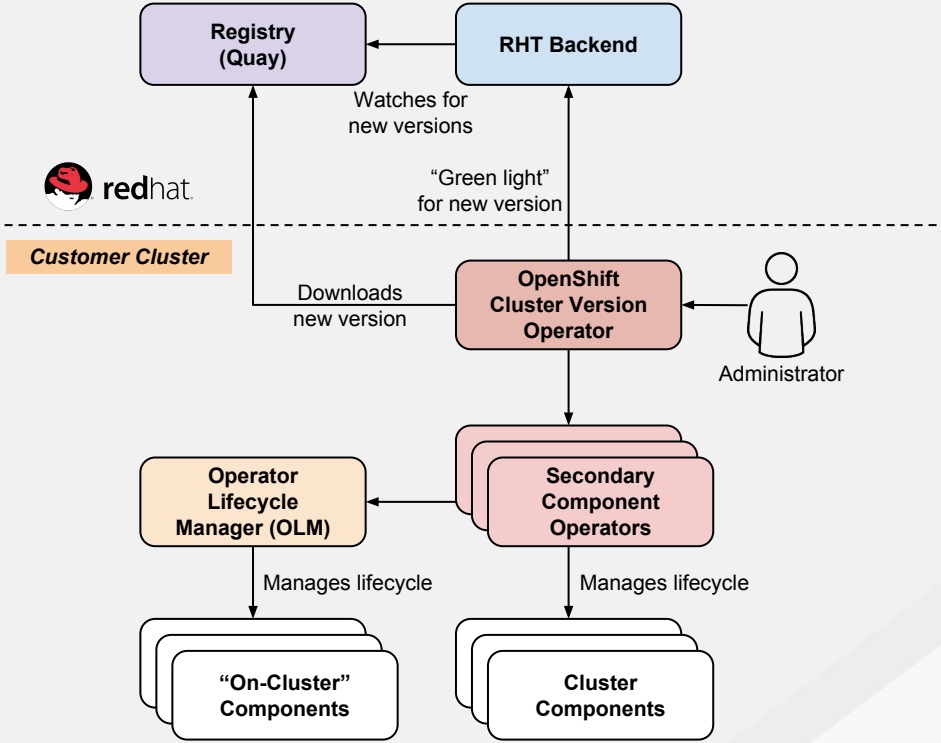


- "Over-The-Air" updates can be driven from either *cloud.openshift.com* or the Cluster Console right on the cluster
- Manual updates will be supported for offline (disconnected) environments
  - Tooling to automate updates will be added in later release

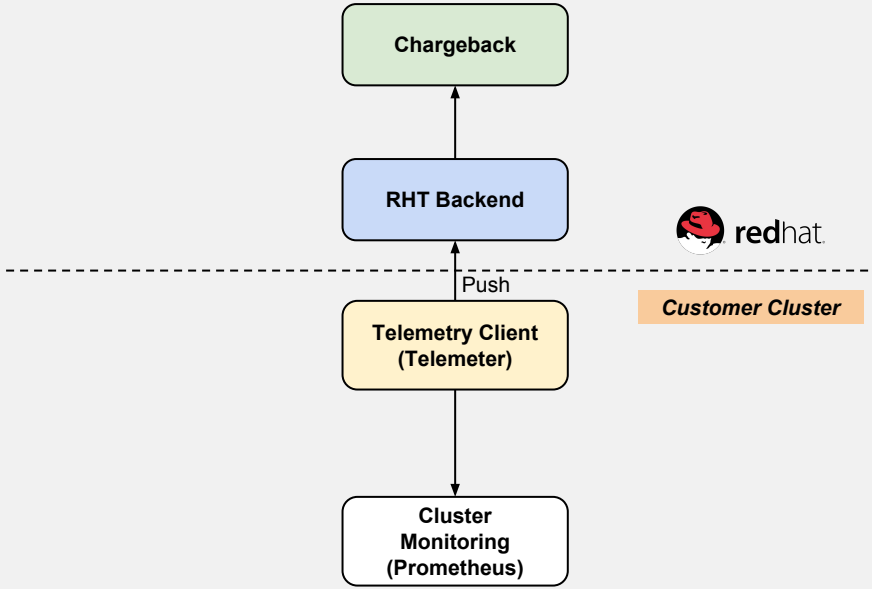
Over-The-Air Updates

How Over-The-Air Updates Work

- RHT backend builds a graph of upgrade possibilities from release images in registry
- OpenShift clusters tell RHT backend who they are and what version it's running
- Policy engine combines information from customer entitlement and upgrade graph to tell clusters what they can upgrade to
- Either an administrator or automatic update controller will edit the Cluster Version Operator's CR with the update version
- Cluster Version Operator will get release image from registry and apply the changes



Connected Customer Telemetry



Insight into Updates & Customer Success

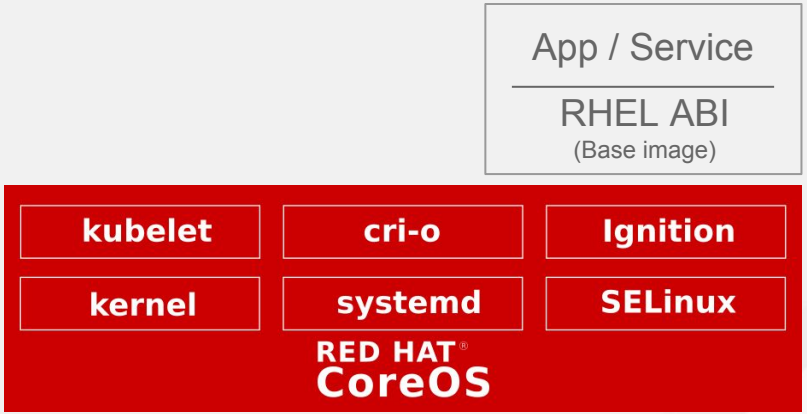
- Customer clusters send metrics back to Red Hat, which is scraped with Prometheus and pushed by Telemeter
- Centralized metrics will be used for:
  - **OTA Updates** - Exceeding failure thresholds will stop the rollout of a given release
  - **SRE / CEE** - Is cluster healthy?
  - **Billing** - Chargeback for hourly usage
  - **App Partners** - Operator metering for the Marketplace

Container Host & Runtimes

Red Hat CoreOS

Delivering an automated RHEL experience with OpenShift

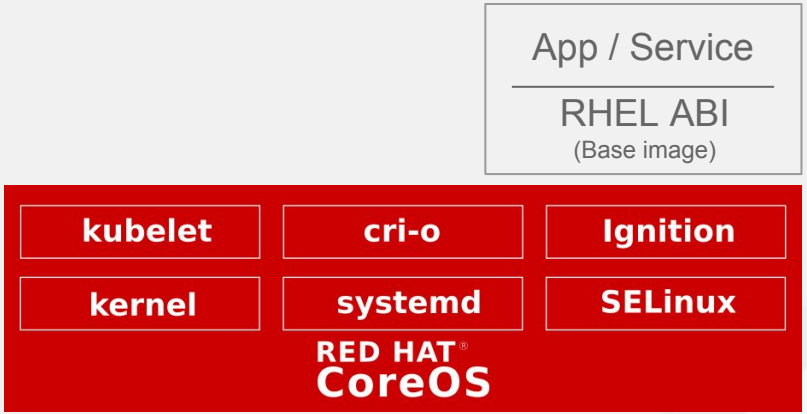
- An immutable host, delivered with OpenShift
  - Aligned lifecycle
  - Aligned release cadence
- Preserving the what matters most from Container Linux
  - Minimal, secure OS with an integrated container stack
  - Automated updates and CVE remediation
  - One-touch provisioning with ignition
- Fully supporting the RHEL ABI and ecosystem



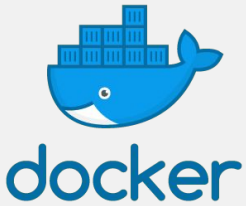
Red Hat CoreOS

Notable Changes

- Kubernetes control plane and clients are moving to the host
- Beta access will be AWS only
  - Other clouds and on-prem will follow shortly after
  - Bare metal is in scope, but host customization may require RHEL
- Moving away from monolithic updates
  - Cluster-aware model, managed by operators and MCD
  - Updates delivered via container images - simple to mirror
- Dropping cloud-init



Container Engine/Runtime Strategy



Experience:

- A lightweight, OCI-compliant container runtime designed for Kubernetes
- Runs any OCI compliant, Docker compatible container images
- Focus on stability and life cycle *with* the platform
- Improve container security & performance at scale

Roadmap

- Now running in production under OpenShift Online clusters
- Graduated from the Kubernetes incubator status - repo move pending
- Continues to track and release with upstream Kubernetes
- On track to become the default container engine for nodes
- Converting node troubleshooting documentation to use crictl for human interface to CRI-O
- Adding user namespace support
- Integrating libpod for better CLI integration with Podman

buildah

Experience

- Will be embedded in OpenShift build strategies, mostly transparent (except custom build strategy)
- OCI Container images compatible with Docker format
- Multi-stage builds supported with and without dockerfiles
- Customizable image layer caching
- Shares the underlying image and storage components with CRI-O

Roadmap :

- GA support with RHEL 7.5
- User namespace enablement
- Working towards unprivileged, non-root container builds
- Future integrations with Ansible (new work on Ansible Builder), and OSBS

podman

Experience

- Provides a familiar command line experience compatible with the docker cli
- Great for running, building, and sharing containers outside of OpenShift
- Can be wired into existing infrastructure where the docker daemon/cli are used today
- Simple command line interface, no client-server architecture, so more agile in many use cases

Roadmap:

- GA in RHEL 7.6 & RHEL 8
- Run containers as non-root (enhanced user namespaces)
- Docker compatible health checks
- Atomic run label support

Summary

OpenShift 4 on Red Hat CoreOS

- CRI-O & Buildah supported exclusively

OpenShift 4 on Red Hat Enterprise Linux 8

- CRI-O & Buildah supported exclusively

OpenShift 4 on Red Hat Enterprise Linux 7

- CRI-O & Buildah is default

Summary

OpenShift 4 on Red Hat CoreOS

- CRI-O & Buildah supported exclusively

OpenShift 4 on Red Hat Enterprise Linux 8

- CRI-O & Buildah supported exclusively

OpenShift 4 on Red Hat Enterprise Linux 7

- CRI-O & Buildah is default
- Fallback support for docker 1.13 - will be removed in later OpenShift dot release

Virt-based Containers

What is the future for KVM isolated containers?

- Lots of interest from customers in this area
- All of these solutions have limitations, compatibility issues, and are not mature enough to support
- Customers seem to get less excited as they learn about the gaps
- Not mature enough to be on our product roadmaps
- Kata seems to be the most promising solution and community
    - We are engaged upstream and currently bringing kata into Fedora

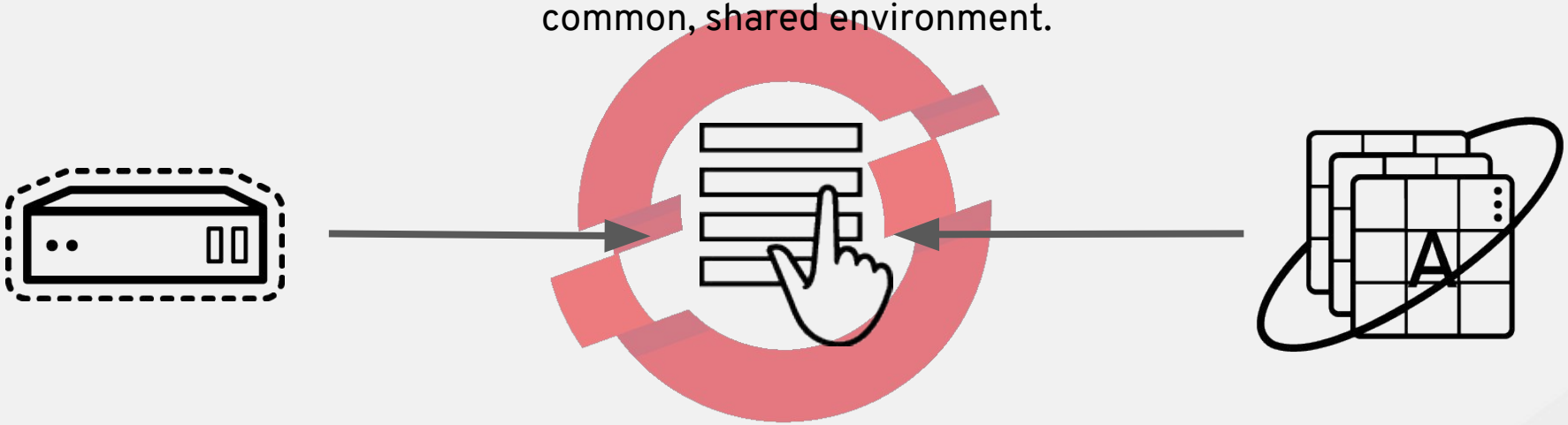
katacontainers

gVisor

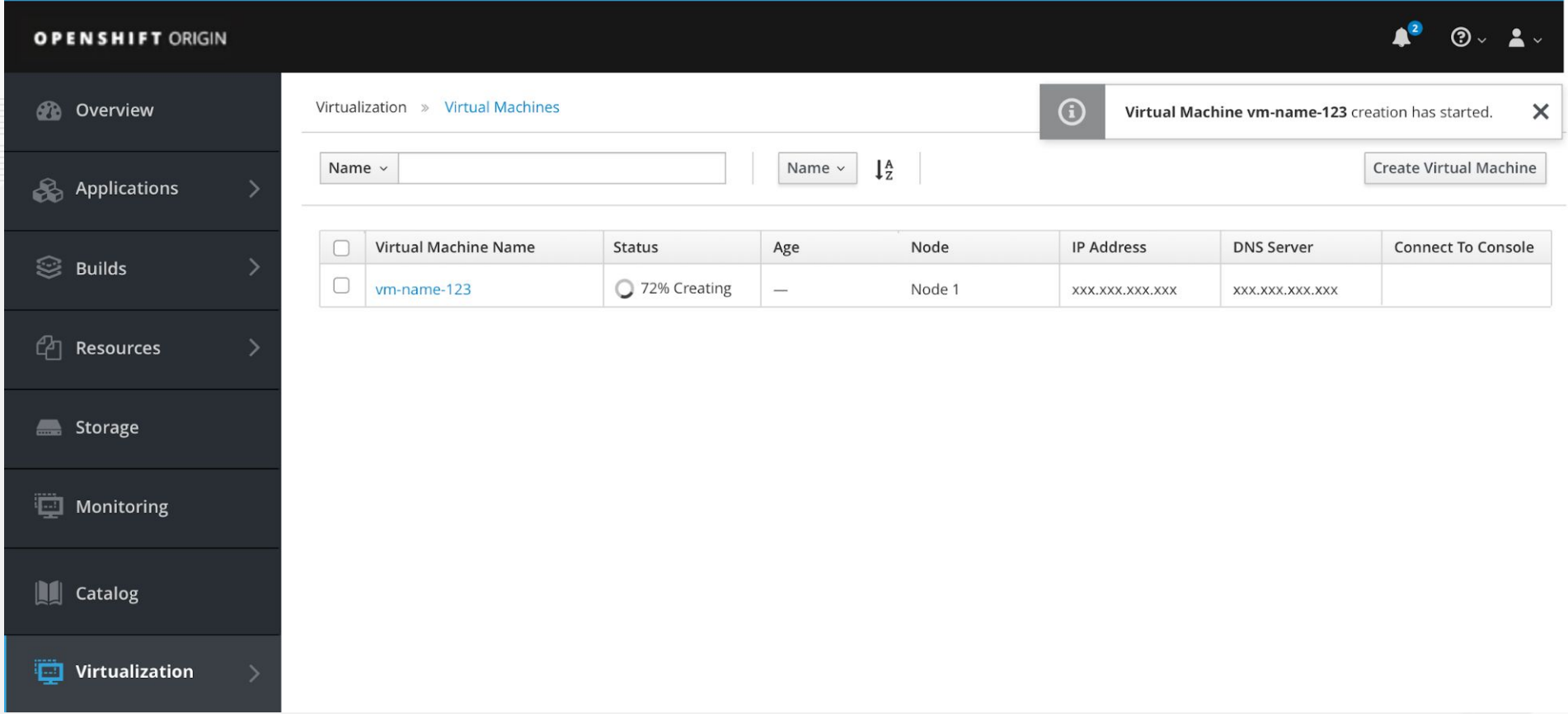
Container-native Virtualization

INTRODUCING
CONTAINER-NATIVE VIRTUALIZATION

Technology enabling developer use of OpenShift as a unified platform for building, modifying, and deploying applications residing in both containers and virtual machines in a common, shared environment.



Add Virtual Machines to your OpenShift projects as easily as Application Containers!



Leverages tried and trusted RHEL & RHV (KVM) virtualization capabilities.

Technology Preview access on an upcoming release of OpenShift Container Platform.

CONTAINER-NATIVE VIRTUALIZATION

Components

KubeVirt (http://kubevirt.io/)

- Kubernetes Virtualization API and runtime in order to define and manage virtual machines.
- Implemented as **CustomResourceDefinitions**.

Containerized Data Importer (https://github.com/kubevirt/containerized-data-importer)

- Data Import Service for kubernetes, designed with kubevirt in mind.

CSI/Ember (https://github.com/Akrog/ember-csi)

- Multi-vendor CSI plugin supporting over 80 traditional storage drivers.
- Extends options beyond existing volume drivers and immediately available CSI options.
- Not all of these drivers will be available/supported immediately.

CONTAINER-NATIVE VIRTUALIZATION

- Currently remain in **developer preview** mode. **Limited** availability, **no** support.

- Working hard with “customer 0” mostly around performance related tuning of guest workloads. Pursuing other production VM workload and productization gaps.

- Technology Preview MVP gating on:
  - Import RHEL/Windows image from URL for direct instantiation or as template.
  - Creation and attachment of L2 network.
  - Creation of VM from template, image, or PXE.
  - Exposure of RDP, VNC (no SPICE) and workload connectivity.
  - Basic VM “knobs” - CPU/RAM.
  - UI exposure of VM creation workflows.

IBM

OCP for POWER 8 & POWER 9 SUPPORT

Introducing support of OCP for ppc64le on September 27

- First release of Openshift for a non-x86 architecture
- Joint development/testing effort with Multi-Architecture team & IBM
- Lifecycle parity w/ OCP for x86 (same EOL)
- Includes prioritized containers in the Red Hat Containers Catalog from the following products (w/ more coming in OCP 3.11 or as the individual products release):
  - RHEL
  - RH OCP
  - RH OSP
  - RH Software Collections
  - RH Developer Toolset

MULTIPLE ARCHITECTURE GROUP
RED HAT

* For more details contact Bronce McClain and Scott Herold

Supporting IBM Middleware on ICP + OpenShift

IBM & Red Hat will provide end-to-end support for Red Hat Certified Containers

	Ad hoc Client created containers	Certified IBM Cloud Paks on ICP + OpenShift
Deployment/Orchestration (Helm Chart)	⚠	☑ ICP, Supported by IBM
IBM Software (core product functionality)	☑ Supported	☑ Supported by IBM
Base OS container image	⚠	☑ RHEL, Supported by Red Hat
Platform Services (logging, monitoring, etc)	⚠	☑ ICP, Supported by IBM ☑ OpenShift, Supported by Red Hat
Cloud Platform (Kubernetes+)	⚠	☑ OpenShift, Supported by Red Hat
Container Host & Infrastructure	⚠	☑ RHEL, Supported by Red Hat

OpenShift Roadmap

Q2 CY2018

OpenShift Container Platform 3.10 (July)

- Kubernetes 1.10 and CRI-O option
- Smart Pruning
- Istio (Dev Preview)
- oc client for developers
- Control plane as static pods and TLS bootstrapping
- Windows Server Containers (Dev Preview))
- Prometheus Metrics and Alerts (Tech Preview)
- S3 Svc Broker

OpenShift Online & Dedicated

- Dedicated self-service: RBAC, limit ranges
- Dedicated encrypted storage, multi-AZ, Azure beta

Q3 CY2018

OpenShift Container Platform 3.11 (Oct)

- Kubernetes 1.11 and CRI-O option
- Infra monitoring, alerting with SRE intelligence, Node Problem Detector
- Etcd and Prometheus Operators (Tech Preview)
- Operator Certification Program and JBoss Fuse Operator
- P-SAP features
- Metering and Chargeback (Tech Preview)
- HPA Custom Metric
- OLM & Operator Framework (Tech Preview)
- New web console for developers and cluster admins
- Ansible Galaxy ASB support
- CNV (Tech Preview)
- OVN (Tech Preview for Windows)
- FISMA Moderate, ISO27001 PAGs, PCI-DSS Reference Architecture

OpenShift Online & Dedicated

- OpenShift Online automated updates for OS
- Chargeback (usage tracking) for OpenShift Online Starter

Q1 CY2019

OpenShift Container Platform 4.0 (March)

- Kubernetes 1.12 and CRI-O default
- Converged Platform
- Full Stack Automated Installer
  - AWS, OSP (tentative)
- Over-The-Air Updates
- RHCC integrated experience
- Windows Containers Tech Preview
- Easy/Trackable Evaluations
- Red Hat CoreOS as immutable host option
- Cluster Registry
- HPA metrics from Prometheus
- FIPS mode for golang (Dev preview)
- OVN Tech Preview

OpenShift Online & Dedicated

- Cluster Operator driven installs
- Self-Service Dedicated User Experience

Q2 CY2019

OpenShift Container Platform 4.1 (July)

- Kubernetes 1.13 and CRI-O default
- Full Stack Automated Installer
  - OSP, Azure
- Istio GA
- Mobile 5.x
- Serverless (Tech Preview)
- RHCC for non-container content
- Integrated Quay (Tech Preview)
- Idling Controller
- Federated Ingress and Workload Policy
- OVN GA
- Che (Tech Preview)

OpenShift Online & Dedicated

- OpenShift.io on Dedicated (Tech Preview)

redhat.

Questions?